PRAKTIJKGIDS MEDISCHE INFORMATIETECHNOLOGIE

EEN INITIATIEF VAN DE KOEPEL MEDISCHE TECHNOLOGIE

PRAKTIJKGIDS MEDISCHE INFORMATIETECHNOLOGIE

HOE SOFTWAREAPPLICATIES, SOFTWARE GESTUURDE MEDISCHE SYSTEMEN MAAR OOK ZELFONTWIKKELDE MEDISCHE SOFTWARE VEILIG EN BETROUWBAAR KUNNEN WORDEN TOEGEPAST.

EEN INITIATIEF VAN DE KOEPEL MEDISCHE TECHNOLOGIE - 2018

VZI: Vereniging van Ziekenhuisinstrumentatietechnici
NVKF: Nederlandse Vereniging voor Klinische Fysica
BMTZ: Biomedisch Technologen in de Zorg
NVKI: Nederlandse Vereniging voor Klinische Informatica
NVKFM: Nederlandse Vereniging van Klinisch Fysisch Medewerkers
WIBAZ: Werkgroep Instrumentatie Beheer Academische Ziekenhuizen

VOORWOORD

Deze Praktijkgids is op initiatief van de Koepel Medische Technologie tot stand gekomen.
De aanleiding om deze gids samen te stellen waren de vele vragen uit het werkveld van de Koepel Medische Technologie. Hoe moeten softwareapplicaties, software gestuurde medische systemen maar ook zelfontwikkelde medische software veilig en betrouwbaar worden geïmplementeerd en toegepast?
Op 11 november 2015 is in Grand Hotel Wientjes in Zwolle de startbijeenkomst geweest waarbij de bij de Koepel aangesloten beroepsverenigingen aanwezig waren. De afgevaardigden van deze verenigingen hebben hun deskundigheid ingebracht op het gebied van de medische informatietechnologie. Op deze bijeenkomst werd duidelijk dat een praktijkgids waarin via diverse praktijkgerichte oplossingen een handreiking wordt geboden, in een behoefte zal voorzien.
Er is vervolgens een werkgroep opgericht die in de brede context van de medische informatietechnologie deze Praktijkgids heeft samengesteld.
De meeste redactievergaderingen hebben plaatsgevonden bij Axioma in Baarn, thuisbasis van de Koepel Medische Technologie. De leden van de werkgroep hebben veel tijd en energie gestoken in het opstellen van de Praktijkgids, wat na twee jaar geleid heeft tot een conceptversie die klaar was voor een redactionele bewerking. Na deze bewerking is de Praktijkgids aan de leden van de beroepsverenigingen voorgelegd met de vraag of de gids aan de verwachting voldoet. Het commentaar van de leden hebben we verwerkt in deze uiteindelijke versie.

Met trots kijk ik terug op de professionaliteit, toewijding en doorzetting van de leden die de Praktijkgids tot stand hebben gebracht. In het bijzonder wil ik hier Joost Ansems noemen. Joost was een actief en betrokken lid van de werkgroep en hij heeft met veel toewijding meegewerkt aan de totstandkoming van de Praktijkgids. Met zijn juridische kennis heeft Joost een belangrijke bijdrage geleverd. Joost is op 27 november 2017 overleden.

Deze Praktijkgids is een prachtig resultaat van multidisciplinaire samenwerking tussen de verenigingen van de Koepel. We vertrouwen erop dat de gids aan de behoefte van het werkveld voldoet.

Henk Imming, *Voorzitter werkgroep (VZI)*

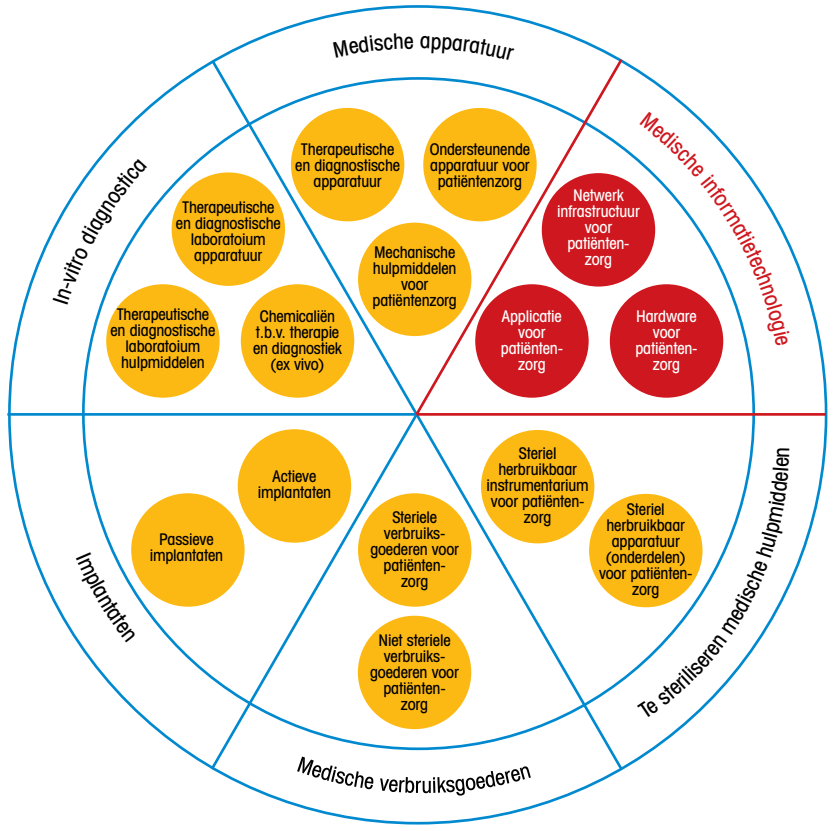
De werkgroep is samengesteld uit:
Joost Ansems, *UMCU (VZI)*
Thierry Felkers, *Radboudumc (NVKI)*
Leo Groenendaal, *Erasmus MC (WIBAZ)*
Vera Lagerburg, *OLVG (NVKF)*
Koos van Ringelenstein, *UMCG (VZI)*
Dagmar Rosenbrand, *LUMC (BMTZ)*
Egon Scheepers, *Amphia (NVKF)*
Wilco Schillemans, *Erasmus MC (NVKF)*
Jannis Syntychakis, *Isala (VZI)*
Dave Wauben, *UMCG (NVKFM)*

INHOUDSOPGAVE

DE PRAKTIJKGIDS IS BEDOELD VOOR DE PROFESSIONALS DIE VANUIT HET TECHNISCH PERSPECTIEF SOFTWARE ONTWIKKELEN, BETROKKEN ZIJN BIJ DE VERWERVING EN/OF EEN ROL HEBBEN IN DE INSTAND-HOUDING, HET GEBRUIK EN DE AFSTOTING VAN DE MEDISCHE INFORMATIETECHNOLOGIE.

1 | INLEIDING

Medische informatietechnologie (zie figuur 1.1) speelt een steeds belangrijkere rol binnen de zorginstellingen. We hanteren hierbij de definitie zoals genoemd in het Convenant Veilige Toepassing Medische Technologie, waarbij het alleen gaat om medische informatietechnologie met een medische toepassing zoals gedefinieerd in de Nederlandse Wet op de medische hulpmiddelen en de Europese Medical Device Directive (MDR). Deze technologie kent verschillende verschijningsvormen en in deze Praktijkgids hebben we verschillende voorbeelden opgenomen. Om deze technologie veilig te kunnen implementeren en te kunnen toepassen, moeten er voor de verschillende componenten op verschillende momenten in de levenscyclus maatregelen worden genomen om alle risico's te beheersen. Alleen zo kunnen we de continuïteit, betrouwbaarheid en patiëntveiligheid borgen. Dit brengt allerlei praktische vragen met zich mee. In de Praktijkgids gaan we aan de hand van praktijkvoorbeelden en toelichtingen uitgebreid in op het onderwerp, waarbij de levenscyclus van deze technologie als uitgangspunt dient. Binnen de context van de medische informatietechnologie komen niet alleen de softwareapplicaties aan de orde maar ook de embedded software op medische apparatuur en de medische systemen, inclusief de daarbij benodigde netwerkinfrastructuur en hardware. De Praktijkgids is bedoeld voor de professionals die vanuit het technisch perspectief software ontwikkelen, betrokken zijn bij de verwerving en/of een rol hebben in de instandhouding, het gebruik en de afstoting van de medische informatietechnologie.



Figuur 1.1 De verschillende categorieën medische hulpmiddelen zoals gedefinieerd in het Convenant, waarbij deze Praktijkgids gaat over de categorie medische informatietechnologie

GEEN VELDNORM

In de Praktijkgids geven we voorbeelden van hoe een ziekenhuis in een specifieke situatie omgaat met medische informatietechnologie. De gids is niet bedoeld als veldnorm voor medische informatietechnologie. Wel willen we verdere bewustwording creëren bij de ziekenhuizen en de leveranciers in de naleving van de vigerende wet- en regelgeving en de toepassing van risicomanagement voor medische informatietechnologie.
Dit document is ontstaan vanuit een initiatief van de bij de Koepel Medische Technologie aangesloten beroepsgroepen. Primair wil de werkgroep met dit document een handreiking geven voor het domein van medische informatietechnologie. Voor de invoering en borging blijft een eigen interpretatie van de handreikingen nodig, deze gids is geen gebruiksklare formule en beschrijft geen werkwijzen met gegarandeerde successen. Deze handreiking mag dan ook niet normatief worden opgevat.

DE REIKWIJDTE EN GEHANTEERDE DEFINITIES

De Praktijkgids is gericht op medische informatietechnologie waaronder softwareapplicaties, embedded software op medische apparatuur en medische systemen en ook de daarbij benodigde netwerkinfrastructuur en hardware bedoeld voor diagnostiek, therapie, ondersteuning van het zorgproces, monitoring van vitale parameters en in-vitro-onderzoek van specimens van patiëntenmateriaal.
Daar waar we spreken over CE-markering bedoelen we CE volgens de Medical Device Directive (MDD) of de Medical Device Regulation (MDR), de In Vitro Medical Device Directive (IVDMD), de In Vitro Medical Device Regulation (IVDR) of de Active Implantable Medical Device Directive (AIMDD).

Wanneer is medische informatietechnologie een medisch hulpmiddel?
Medische informatietechnologie is een medisch hulpmiddel als deze voldoet aan de definitie van een medisch hulpmiddel zoals deze is vastgelegd in de Wet op de medische hulpmiddelen. Een medisch hulpmiddel is:

‘elk instrument, toestel of apparaat, elke software of stof of elk ander artikel dat of die alleen of in combinatie wordt gebruikt, met inbegrip van de software die door de fabrikant speciaal is bestemd om te worden gebruikt voor diagnostische en/of therapeutische doeleinden en voor de goede werking ervan benodigd is, door de fabrikant bestemd om bij de mens te worden aangewend voor:

- diagnose, preventie, bewaking, behandeling of verlichting van ziekten;
- diagnose, bewaking, behandeling, verlichting of compensatie van verwondingen of een handicap;
- onderzoek naar of vervanging of wijziging van de anatomie of van een fysiologisch proces;
- beheersing van de bevruchting, waarbij de belangrijkste beoogde werking in of aan het menselijk lichaam niet met farmacologische of immunologische middelen of door metabolisme wordt bereikt, maar wel door dergelijke middelen kan worden ondersteund.’

(Bron: Medical Device Directive (MDD), Medical Device Regulation (MDR))

Gehanteerde definities

- Medische informatietechnologie: standalone software en apps, software op medische apparatuur en medische systemen (inclusief bijbehorende IT-infrastructuur) waarvan het beoogd gebruik binnen de definitie van MDR/MDD valt;
- Medische software: standalone software en medische apps waarvan het beoogd gebruik binnen de definitie van MDR/MDD valt;
- Medische apparatuur: apparatuur waarvan het beoogd gebruik binnen de definitie van MDD/MDR, IVDMD/IVDR of AIMDD/MDR valt. Deze kan ook software bevatten (embedded software);
- Medische systemen: medische apparatuur gekoppeld binnen een IT-infrastructuur.

In de Praktijkgids spreken we over medische informatietechnologie. Daar waar nodig gebruiken we specifiek de term medische software of medisch systeem.

LEESWIJZER

De redactie heeft getracht de Praktijkgids zodanig in te richten dat de lezer doelgericht zijn informatie kan vinden. De lezer kan al naar gelang van behoefte de gids van A tot Z lezen, zich verdiepen in een casus in hoofdstuk 3 of de gids openslaan bij een specifieke vraag in hoofdstuk 4. We zijn ons ervan bewust dat de tekst door deze opzet her en der overlap vertoont, maar omarmen dit omdat we willen dat de bijdragen ook eigenstandig te lezen zijn. Voor de lezer die deze gids niet online leest maar op papier: we verwijzen op sommige plekken naar aparte bijlages die te vinden zijn op de site van MT Integraal.
We hebben deze bijlages niet in de gids opgenomen omdat het omvangrijke bestanden zijn. Sommige bestanden zijn afkomstig uit de interne organisatie van een ziekenhuis en zijn dus niet online te vinden.

Een lijst met alle bijlages staat in hoofdstuk 7 *Lijst met bijlages*.
Overigens hebben we niet alle externe bronnen waar we naar verwijzen in de bijlagen opgenomen. In het merendeel van de voetnoten verwijzen we naar de sites waar de betreffende informatie te vinden is. Dat is een bewuste keus omdat die content aan verandering onderhevig kan zijn.
In hoofdstuk 2 beschrijven we in een gefaseerd stappenplan van de gehele levenscyclus welke acties genomen moeten worden om de medische informatietechnologie veilig te kunnen gebruiken. Het gaat om de initiële fase van ontwikkeling, de verwervingsfase, de fase van ingebruikname, de gebruiksfase en de afstotingsfase.
In hoofdstuk 3 werken we een vijftal praktijkvoorbeelden nader uit volgens deze methodiek. In deze praktijkvoorbeelden van medische informatietechnologie lichten we stapsgewijs per fase in de levenscyclus het veilige en betrouwbare gebruik toe met concrete processtappen. Het wordt daar duidelijk hoe de desbetreffende ziekenhuizen de medische informatietechnologie conform de vigerende wet- en regelgeving in de patiëntenzorg geïmplementeerd hebben, gebruiken en beheren.

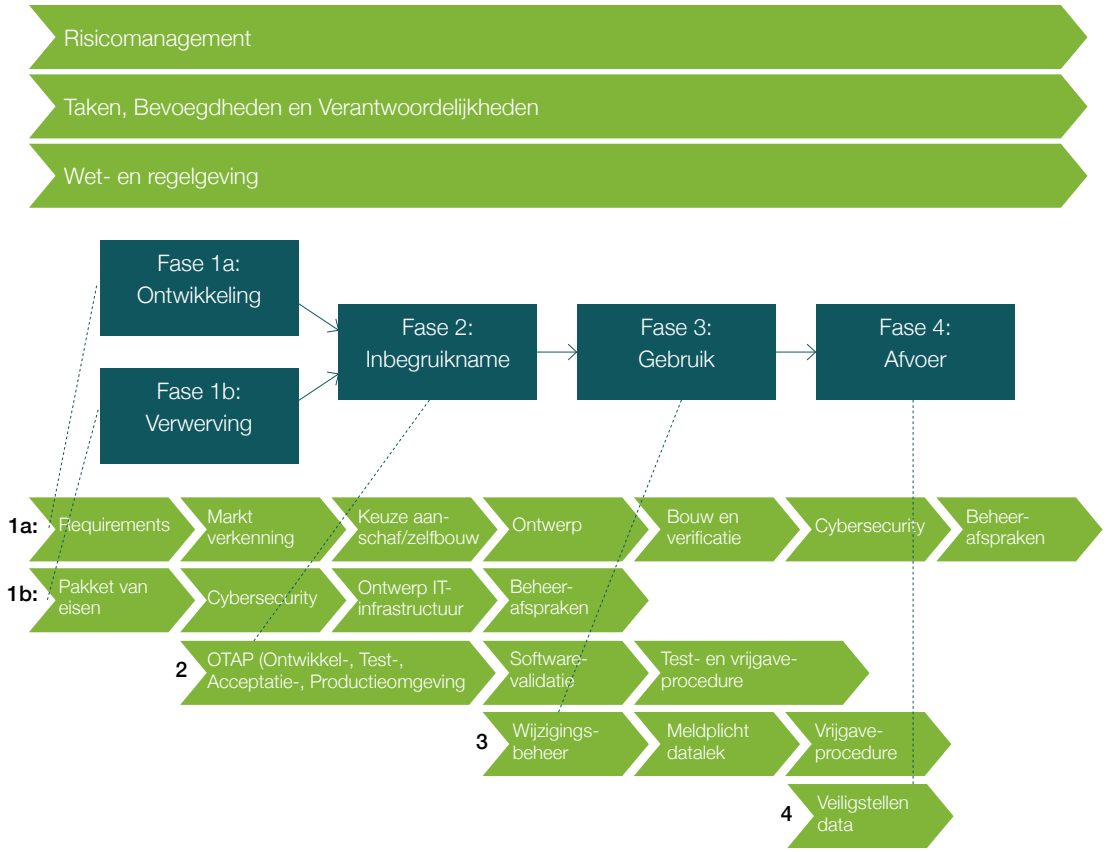
CASUS 1	CASUS 2	CASUS 3	CASUS 4	CASUS 5
Embedded software	Geïntegreerd medisch systeem (binnen één CE aangeboden door een leverancier)	Softwareapplicatie	Zelfbouw software	Medisch systeem
Echotoestel	Ergometrieopstelling	Cardio PACS	TBI	VOS-MOS-MA

In hoofdstuk 4 beantwoorden we veelvoorkomende vragen uit de praktijk die betrekking hebben op het onderwerp van de Praktijkgids.

En in hoofdstuk 5 is er ten slotte ruimte voor discussie omdat we, zoals gezegd, geen veldnorm willen formuleren met deze gids maar wel de bewustwording willen bevorderen van iedereen die met medische informatietechnologie werkt.

2 | LEVENSCYCLUS MEDISCHE INFORMATIETECHNOLOGIE

De levenscyclus van medische informatietechnologie in een zorginstelling kan ingedeeld worden in vier verschillende fasen: verwerving, ingebruikname, gebruik en afvoer. Elke fase kent onderwerpen die op dat moment van toepassing zijn, zoals het opstellen van het Pakket van Eisen tijdens de fase verwerving. Ook zijn er onderwerpen die spelen over de gehele levenscyclus, zoals risicomanagement en Taken, Bevoegdheden en Verantwoordelijkheden. Er zijn ook onderwerpen die meerdere keren in de levenscyclus voorkomen, zoals de test- en vrijgaveprocedure. We bespreken hier de hele levenscyclus en de bijbehorende onderwerpen in het kort. In het hoofdstuk *4 Praktijkvragen* gaan we, zoals gezegd, nader in op specifieke vragen rondom deze onderwerpen.
Figuur 2.1 geeft een goed overzicht van de verschillende fasen en de bijbehorende onderwerpen die in deze Praktijkgids aan bod komen.

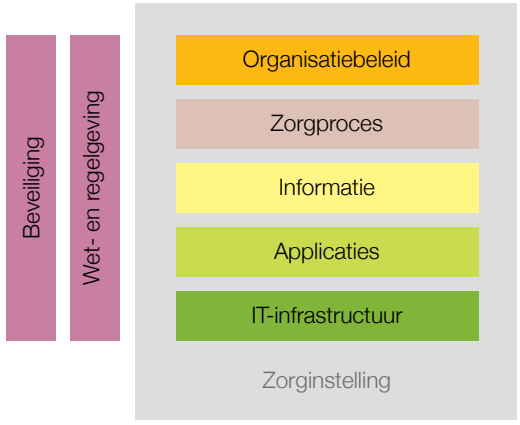


Figuur 2.1 Overzicht van alle fasen in de levenscyclus van medische informatietechnologie inclusief de in de Praktijkgids besproken onderwerpen

In het Convenant vallen verwerving en ingebruikname samen onder de fase ‘invoering’. Wij hebben deze fase opgesplitst in twee delen omdat de fase van ingebruikname een aantal specifieke stappen vereist die in deze Praktijkgids nader worden uitgewerkt. Naast deze vier fasen is het ook mogelijk dat een ziekenhuis zelf medische hulpmiddelen ontwikkelt. Als dit het geval is, begint de levenscyclus bij de fase ontwikkeling.

Het is belangrijk om te beseffen dat in de verschillende fasen van de levenscyclus er bij het implementeren van medische (informatie)technologie niet alleen afspraken moeten worden gemaakt over de techniek. Meestal wordt de technologie in een bestaand zorgproces binnen een bestaande organisatie ingezet en moet de technologie (samen-) werken met andere medische (informatie-) systemen. Het is dan belangrijk dat de nieuwe informatietechnologie ook binnen deze bestaande architectuur functioneert. In de praktijk van informatiemodellen wordt dit ook wel interoperabiliteit genoemd. Een belangrijk model hiervoor is het interoperabiliteitsmodel van Nictiz, zie figuur 2.2. Hierin zijn de verschillende lagen weergegeven van heel

abstract (wetgeving) tot de fysieke componenten (infrastructuur). Dit model is ook het uitgangspunt voor samenwerking tussen verschillende organisaties, maar dat onderwerp valt buiten de scope van deze gids. De kern van de Praktijkgids is dat er op de verschillende lagen afspraken moeten worden gemaakt voor de implementatie van medische informatietechnologie.



Figuur 2.2 Interoperabiliteitsmodel (Bron: Nictiz)

OVERKOEPELENDE PROCESSEN

Sommige processen zijn tijdens de hele levenscyclus van belang:
Risicomanagement, Taken, Bevoegdheden en Verantwoordelijkheden en Wet- en regelgeving. Hieronder staan ze kort beschreven. Zoals in het interoperabiliteitsmodel te zien is, zijn deze processen ook overkoepelend over de verschillende lagen.

Risicomanagement

Onder risicomanagement verstaan we beleid gericht op risicobeheersing, waarbij de veiligheid van patiënten, zorgverleners en bezoekers zo veel mogelijk wordt nagestreefd. Deze definitie impliceert dat zekerheid in de strikte, risicovrije betekenis niet bestaat; het lukt lang niet altijd alle risico's te voorzien. Risicomanagement van medische informatietechnologie wordt door het Convenant zelfs gedurende de gehele levenscyclus voorgeschreven. Daarnaast wordt risicomanagement ook aangeraden vanuit normen en richtlijnen zoals de IEC 80001 (IEC 80001-1 Application of risk management for IT networks incorporating medical devices IEC 80001-2-1 Step-by-step risk management of medical IT-networks) en IEC 80002-1. Vaak wordt aangeraden om risicomanagement volgens de ISO 14971 uit te voeren. Naast deze richtlijnen zijn er ook praktijkrichtlijnen of praktijkgidsen zoals de Leidraad NIKP: nieuwe interventies in de klinische praktijk[1], de praktijkgids Risicomanagement en Medische Technologie van VMSzorg[2] en het WINT2.0 rapport vanuit de Koepel MT over Risicomanagement ten behoeve van veilig toepassen van medische hulpmiddelen[3].
In hoofdstuk 4 *Praktijkvragen* beschrijven we welke methodieken van risicoanalyses er zijn, wat de belangrijkste risico's zijn waarmee men rekening moet houden en hoe men die zo klein mogelijk kan houden.

Taken, Bevoegdheden en Verantwoordelijkheden

Om medische hulpmiddelen veilig toe te passen gedurende de gehele levenscyclus is het noodzakelijk om de Taken (T) Bevoegdheden (B) en Verantwoordelijkheden (V) op een duidelijke manier te beschrijven en binnen de organisatie bij de verschillende actoren te beleggen. In hoofdstuk 4 *Praktijkvragen* komen verschillende methodieken om dit te doen aan bod, inclusief voorbeelden.

Wet- en regelgeving

Er is heel veel wet- en regelgeving die van belang is tijdens de levenscyclus van medische informatietechnologie. De belangrijkste is de Wet op de medische hulpmiddelen. Deze beschrijft wanneer iets een medisch hulpmiddel is en waaraan dit minimaal moet voldoen. Daarnaast zijn er nog normen op bijvoorbeeld het gebied van risicomanagement, het ontwikkelen van software en databeveiliging die van belang zijn voor medische informatietechnologie.

FASE 1A: ONTWIKKELING

Sommige ziekenhuizen ontwikkelen in eigen beheer medische informatietechnologie die onder de definitie van medisch hulpmiddel valt. Vaak worden deze producten alleen binnen de eigen instelling gebruikt, soms worden deze echter ook (al dan niet tegen betaling) aan andere instellingen ter beschikking gesteld. Als dit laatste het geval is, is het ziekenhuis fabrikant geworden en geldt de daarbij behorende wet- en regelgeving. Voordat een ziekenhuis start met zelfbouw moet men eerst goed afwegen of het noodzakelijk is om zelf te ontwikkelen. Is er niet ook een commercieel alternatief voor handen? Vanaf 26 mei 2020 (de ingangsdatum van de nieuwe MDR), respectievelijk 26 mei 2022 voor IVD medische hulpmiddelen, mag zelf ontwikkelen alleen nog als aangetoond kan worden dat er geen product op de markt is dat voldoet aan de gestelde eisen.
Ongeacht de toepassing is de kwaliteit van het geleverde product belangrijk. Om een zeker kwaliteitsniveau te garanderen, bespreken we bij de Praktijkvragen welke stappen doorlopen kunnen worden om zelf software veilig te ontwikkelen. In dat hoofdstuk komt ook de relevante wet- en regelgeving aan bod.
In het kort komt het zelfbouwproces op de volgende stappen neer. Na een marktonderzoek, waaruit de rechtvaardiging voor zelfbouw volgt, wordt een ontwikkelplan geschreven dat alle facetten van het ontwikkeltraject beschrijft. Hierna volgt het programma van wensen en eisen, waarin alle eisen voor het te bouwen systeem worden verzameld. Dit wordt gevolgd door de ontwerpfase, die afhankelijk van de risicoklasse van het te bouwen systeem uit één of meerdere stappen kan bestaan, zoals architectuur en gedetailleerd design. Zie hiervoor de paragraaf over ingebruikname.

FASE 1B: VERWERVING

Verwerving bevat alle acties voor het, al dan niet met behulp van een overeenkomst, ter beschikking krijgen van een medisch hulpmiddel. Er zijn diverse vormen van verwerving zoals aanschaf, lease, huur, (bruik-)leen, consignatie, proefplaatsing en zichtzending.

[1] *Zie bijlage I Leidraad NIKP: nieuwe interventies in de klinische praktijk op www.mtintegraal.nl*

[2] *https://www.vmszorg.nl/praktijkvoorbeelden-en-tools/praktijkgids-risicomanagement-en-medische-technologie/*

[3] *https://www.wibaz.nl/mdocs-posts/wint-2-0-rapport/*

De verwervingsfase start met de behoefte van een gebruiker om voor een bepaalde toepassing medische informatietechnologie aan te schaffen. Daarbij levert de aanvrager een onderbouwing met nut en noodzaak van de beoogde verwerving. We gaan er voor deze Praktijkgids vanuit dat er toestemming is om de beoogde medische informatietechnologie te verwerven. De voorbereiding van de verwerving kan dus starten. De documenten die opgesteld worden tijdens de verwervingsfase moeten vastgelegd worden in het productdossier.[4]
De belangrijkste onderdelen van de verwervingsfase zijn het opstellen van een Pakket van Eisen (PvE), prospectieve risicoanalyse, cybersecurity, het IT-infrastructuurontwerp en de beheerafspraken. Deze onderdelen worden hieronder kort toegelicht.

Pakket van Eisen
Bij iedere verwerving van medische informatietechnologie is het noodzakelijk om een Pakket van Eisen (PvE) op te stellen. Een PvE heeft drie doelen. Allereerst zorgt het ervoor dat eisen en wensen van de diverse betrokken partijen duidelijk zijn en op elkaar afgestemd worden. Daarnaast wordt het gebruikt voor een leveranciersselectie: welke leverancier voldoet het beste aan het opgestelde PvE? Ten derde kan het door de leverancier ingevulde PvE gebruikt worden als onderdeel van het latere koopcontract en een eventuele onderhoudsovereenkomst, waarbij een deel van de afspraken vastligt.
Binnen het ziekenhuis moeten goede afspraken zijn wie er verantwoordelijk is voor het opstellen van het PvE. Om een goed PvE op te stellen is er een multidisciplinaire groep nodig. Bij het opstellen van het PvE is het belangrijk om een goede afweging te maken tussen algemene en specifieke eisen. Bij te algemene eisen zullen alle leveranciers voldoen, bij te specifieke eisen kan het voorkomen dat veel leveranciers afvallen. Eén van de ontwikkelingen binnen het opstellen van een PvE is het maken van een functioneel PvE in plaats van een opsomming van eisen en wensen. Hiermee wordt bedoeld dat vanuit het ziekenhuis de functionele wensen en eisen op papier gezet worden. Zoals: voor welke toepassing is de medische informatietechnologie bedoeld? Op welke afdeling wordt het ingezet? En welke processen moeten ermee ondersteund worden?
Dit biedt meer vrijheid aan de leverancier om aan te bieden wat zij denken dat bij het ziekenhuis past.
Bij het opstellen van de eisen is het zinvol om na te gaan of de afspraken op alle lagen van het Interoperabiliteitsmodel (figuur 2.2) zijn verwoord. Denk bijvoorbeeld aan eisen omtrent het inpassen binnen het beleid van de organisatie, de bestaande workflow en het zorgproces, maar ook eisen in relatie tot bijvoorbeeld de applicatiearchitectuur en bestaande technische infrastructuur.

Cybersecurity
Onder cybersecurity wordt verstaan het vrij zijn van gevaar of schade veroorzaakt door verstoring, uitval of misbruik van IT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de IT, schending van de vertrouwelijkheid van de opgeslagen informatie of schade aan de integriteit van die informatie.
Om de cybersecurity goed te regelen is het noodzakelijk om in de verwervingsfase met de leverancier en de relevante afdelingen binnen het ziekenhuis goede afspraken te maken hoe de nieuwe medische informatietechnologie beveiligd kan worden. Denk hierbij bijvoorbeeld naast de IT-afdeling ook aan de security officer en de functionaris bescherming persoonsgegevens. Cybersecurity komt terug op alle lagen van het Interoperabiliteitsmodel (figuur 2.2) omdat het niet alleen technische maatregelen betreft maar bijvoorbeeld ook het beleid. Diverse wet- en regelgeving, zoals de Algemene verordening gegevensbescherming (AVG), eist van de ziekenhuizen dat ze de cybersecurity goed op orde hebben.

IT-infrastructuurontwerp
Waar in het verleden sprake was van fysiek gescheiden medische en niet-medische IT-netwerk(en), is in de afgelopen jaren een duidelijke trend waarneembaar waarbij ziekenhuizen er steeds meer voor kiezen om ook medische toepassingen gebruik te laten maken van het algemene IT-ziekenhuisnetwerk.
Een belangrijke voorwaarde om het standaardziekenhuisnetwerk te gebruiken voor medische toepassingen is het maken van goede afspraken tussen de afdelingen IT en Medische Techniek. Er is dan namelijk sprake van gedeelde verantwoordelijkheid voor de juiste werking van de keten. Dit is een onderwerp op de infrastructuurlaag van het Interoperabiliteitsmodel (figuur 2.2).
Voor de inrichting van de IT-infrastructuur moeten in de verwervingsfase goede afspraken gemaakt worden met de leverancier. Welke eisen stelt deze aan de infrastructuur, en kan het ziekenhuis daaraan voldoen bij de inrichting van bijvoorbeeld VLAN en wifi-infrastructuur?

Beheerafspraken
Om medische informatietechnologie veilig toe te passen gedurende de gehele levenscyclus is het noodzakelijk om tijdens de verwervingsfase de Taken (T) Bevoegdheden (B) en Verantwoordelijkheden (V) op een duidelijke manier te beschrijven. TBV moeten intern bij de verschillende actoren belegd worden en extern bij de leverancier. Dit laatste kan bijvoorbeeld met behulp van een Standaard Service Overeenkomst (SSO) van de WIBAZ[5], of met een SLA. Een SLA (Service Level Agreement) is een overeenkomst tussen een opdrachtgever en een leverancier (intern of extern) waarin afspraken worden opgenomen over de diensten of producten die een leverancier aan de opdrachtgever levert, met welk kwaliteitsniveau en tegen welke kosten.
De afspraken moeten zodanig zijn ingeregeld dat er tijdens het gebruiksproces een goede storingsprocedure en wijzigingsproces zijn ingericht. Vanuit de MDR gezien, moet de leverancier een werkende post market surveillance en een recall procedure hebben.
Voor een goed service management is het van belang om de gemaakte afspraken regelmatig te evalueren aan de hand van rapportages over de geleverde prestaties.
De beheerafspraken worden gemaakt op de laag Organisatiebeleid van het Interoperabiliteitsmodel (figuur 2.2).

FASE 2: INGEBRUIKNAME

De fase ingebruikname loopt vanaf het moment van de verwerving tot de klinische ingebruikname. In deze fase worden alle voorbereidingen voor de gebruiksfase getroffen. Zo moet het product getest worden en moeten de gebruikers en beheerders getraind worden. Pas daarna volgt uiteindelijk de vrijgave.

[4] *https://www.vmszorg.nl/medische-technologie/convenant-medische-technologie/*

[5] *Zie het formulier op de site van WIBAZ https://www.wibaz.nl/mdocs-posts/standaard-service-overeenkomst-2016/*

OTAP
Om het product te kunnen testen en te valideren wordt vaak een OTAP-omgeving ingericht. Dit acroniem staat voor:

- Ontwikkelomgeving (meestal alleen bij de fabrikant)
- Testomgeving (onderdeel van de initiële installatie)
- Acceptatieomgeving (een recente kopie van de Productieomgeving inclusief de koppelingen)
- Productieomgeving (de uiteindelijke productieomgeving)

Deze omgevingen zijn virtueel en/of fysiek van elkaar gescheiden.
Voor validatie/verificatie van medische systemen is het noodzakelijk om naast de productie (klinisch gebruik) ook een acceptatieomgeving beschikbaar te hebben. Het is belangrijk dat de acceptatieomgeving een representatieve kopie van de productieomgeving is. Denk dus ook aan de gekoppelde randapparatuur en/of de interne en externe datakoppelingen.
Bij het inrichten van een OTAP-omgeving hoort ook een wijzigingsproces om gedurende de levensduur van de medische informatietechnologie, de kwaliteit goed te borgen. De geldende afspraken op de applicatie- en infrastructuurlaag van het Interoperabiliteitsmodel (figuur 2.2) moeten daarbij in acht worden genomen.

Vrijgaveprocedure
Wanneer het installeren, configureren, testen en valideren met succes is afgerond volgt de vrijgaveprocedure. De vrijgave kan onderverdeeld worden in een technische en functionele vrijgave. De technische vrijgave geeft aan dat de medische informatietechnologie technisch functioneert en vrijgegeven wordt door de beheerder/ deskundige aan de gebruiker. De functionele vrijgave wordt bij voorkeur door een gebruiker gedaan en geeft aan dat de technologie klinisch gebruikt mag worden. Op het moment van klinische ingebruikname moet de gebruiker dus ook getraind zijn.
Vrijgave vindt plaats op drie verschillende momenten binnen de levenscyclus: bij de ingebruikname van nieuwe technologie en in de gebruiksfase na (preventief en correctief) onderhoud en na het doorvoeren van wijzigingen.
Voor de formele overdracht van technologie aan de afdeling/gebruiker kan men een standaard overdrachtsformulier gebruiken (bijlage II).[6]

FASE 3: GEBRUIK

In deze fase is de medische informatietechnologie in gebruik genomen. Deze fase omvat periodiek en correctief onderhoud, modificaties, bij- en nascholing, evaluaties en recall- en veiligheidsmeldingen.

Wijzigingsbeheer of modificaties?
Net als bij de beheerafspraken in de verwervingsfase moeten op de beleidslaag van het Interoperabiliteismodel (figuur 2.2) ook in de gebruiksfase goede afspraken worden gemaakt. De leverancier van software kan periodiek nieuwe versies van zijn software uitbrengen. Dit kunnen versies met vernieuwde functionaliteit zijn (upgrades), maar ook met oplossingen voor (risicovolle) problemen(updates). Een leverancier kan in dat geval de gebruiker verplichten de nieuwe versie van de software in gebruik te nemen.
Bij een grote upgrade wordt er vanuit deze fase weer teruggegaan naar de verwervings- of ingebruiknamefase. Naar welke fase wordt teruggegaan hangt van een aantal zaken af. Als er een afweging gemaakt moet worden of de upgrade wel of niet uitgevoerd moet worden is het verstandig om terug te gaan naar de verwervingsfase, waarbij wederom alle interne partijen in het ziekenhuis (gebruikers en beheerorganisatie) betrokken worden.
Er kan dan op basis van een PvE, de release notes van het product en een risicoanalyse een keuze gemaakt worden voor wel of niet implementeren van de upgrade. Als het een verplichte upgrade is, wordt alleen de fase ingebruikname doorlopen. In het geval van zelfbouw moet men teruggaan naar de ontwikkelfase.

De aangepaste versie moet in de verschillende beschikbare OTAP-omgevingen worden geïmplementeerd en getest. Deze testen kunnen zowel technisch als functioneel van aard zijn. Functioneel gaat het dan om de werking en het gebruik van de software zelf. Technisch moet worden gedacht aan het testen van koppelingen en de integratie met andere systemen, aan performance-testen en veiligheidstesten.
Tijdens het uitvoeren van een wijziging liggen de verantwoordelijkheden bij de betrokkenen zoals is vastgelegd in de diverse interne beleidsstukken of overeenkomsten (TBV, SLA, SSO). Deze zijn zo wel op in- als externe samenwerkingen gericht.

Vrijgaveprocedure
Afhankelijk van de impact van het periodiek of correctief onderhoud inclusief eventuele modificaties, kan men kiezen voor een beperkte set van technische en functionele testen ten opzichte van de testen bij ingebruikname. De vrijgave zelf vindt op dezelfde manier plaats als in de fase van ingebruikname, ook weer met de tweedeling in technische en functionele vrijgave.

Datalek
Sinds 1 januari 2016 geldt de meldplicht datalekken. Dit houdt in dat een organisatie zoals het ziekenhuis direct een melding moet doen bij de Autoriteit Persoonsgegevens zodra er een ernstig datalek is.[7] Het gaat dan om tot een persoon herleidbare data.
De meldplicht datalekken is ook van toepassing bij medische informatietechnologie. Rondom medische informatietechnologie hebben we voornamelijk te maken met patiëntgegevens en deze data mogen niet in handen van onbevoegde personen vallen.

FASE 4: AFSTOTING

Tijdens de afstotingsfase wordt de medische informatietechnologie afgekeurd, buiten gebruik gesteld en afgevoerd. Hierbij zijn een aantal zaken van belang:

- buiten bedrijf stellen software;
- veiligstellen data, via conversie of via data warehouse;
- verwijderen data;
- beëindigen servicecontract en/of licentieovereenkomst.

Bij afvoer van medische informatietechnologie moeten de data die daarop staan veiliggesteld worden en daarna verwijderd worden van het apparaat. Ingeval de data niet verwijderd kunnen worden door het ziekenhuis zelf moet het ziekenhuis met de leverancier een vernietigingsverklaring opstellen en gezamenlijk ondertekenen. Daarmee wordt de verantwoordelijkheid om de patiëntgegevens te verwijderen overgedragen naar de leverancier.
De afstoting is een voorbeeld van een onderwerp op onder andere de informatielaag van het Interoperabiliteitsmodel (figuur 2.2). De daadwerkelijke afvoer valt buiten de scope van de Praktijkgids, valt buiten scope, maar kan worden opgenomen in een vernietigingsverklaring.

[6] *Zie bijlage II Standaard overdrachtsformulier op www.mtintegraal.nl*

[7] *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken*

AFHANKELIJK VAN DE SITUATIE KUNNEN WE MEDISCHE INFORMATIETECHNOLOGIE INDELEN IN VIJF CATEGORIEËN. IN DE PRAKTIJK BLIJKT DEZE INDELING NIET ALTIJD EENDUIDIG. WE HEBBEN DAAROM EEN AANTAL HERKENBARE PRAKTIJKVOORBEELDEN UITGEWERKT WAARMEE WE EEN GROOT DEEL VAN DE CATEGORIEËN BESCHRIJVEN, MAAR WE PRETENDEREN HIERMEE NIET OM ALLES VOLLEDIG AFGEDEKT TE HEBBEN.

3 | VOORBEELDEN UIT DE PRAKTIJK

Medische informatietechnologie als medisch hulpmiddel kan in de praktijk in verschillende categorieën worden onderverdeeld. In dit hoofdstuk hebben we voor elk van deze categorieën toegelicht hoe de medische informatietechnologie gedurende de levenscyclus veilig in de specialistische patiëntenzorg kan worden toegepast.
Het Convenant onderscheidt binnen de informatietechnologie drie categorieën. In deze Praktijkgids hanteren we de volgende onderverdeling met vijf categorieën:

- Embedded software
- Geïntegreerd medisch systeem (binnen één CE aangeboden door een leverancier)
- Softwareapplicatie (ook medische apps en Software as a Service)
- Medisch systeem
- Zelfbouw software

Afhankelijk van de situatie kunnen we medische informatietechnologie indelen in een van bovenstaande categorieën. In de praktijk blijkt het niet altijd eenduidig. In dit hoofdstuk hebben we daarom een aantal herkenbare praktijkvoorbeelden uitgewerkt waarmee een groot deel van de categorieën is beschreven, maar we pretenderen hiermee niet om alles volledig afgedekt te hebben. In de praktijk kunnen andere situaties/configuraties leiden tot discussie, maar hopelijk geven de voorbeelden voldoende richting en handvatten om de vragen te beantwoorden.
Elk praktijkvoorbeeld begint met een globale beschrijving, vervolgens belichten we de diverse overwegingen die in de praktijk gemaakt moeten worden. We sluiten elk praktijkvoorbeeld af met een casus vanuit de praktijk van een zorginstelling waarin we de aandachtspunten per fase in de levenscyclus van medische informatietechnologie concreet maken. Dit zijn dus slechts voorbeelden hoe dit in specifieke zorginstellingen is uitgewerkt.

We beschrijven in de voorbeelden de volgende aspecten:

- Wet- en regelgeving
- Systeem specificaties/PvE
- Security
- IT-infrastructuur
- Beheerafspraken
- Test- en vrijgaveprocedure
- Wijzigingsbeheer
- Afstotingsprocedure

ECHO

Echotoestellen worden toegepast voor de diagnostiek in bijvoorbeeld de cardiologie, verloskunde en radiologie. De ultrageluidtechnologie heeft de afgelopen decennia een grote ontwikkeling doorgemaakt, zo is inmiddels het maken van real-time 3D kleurenbeelden mogelijk. Vanwege deze ontwikkelingen is er een steeds grotere rol voor informatietechnologie in deze toepassing.
Het besturingssysteem dat in het echotoestel wordt toegepast is een embedded Operating System (OS). Dit besturingssysteem dient primair als applicatieplatform voor de software die zorgt voor het aansturen van het echotoestel en secundair voor de communicatie van de patiëntinformatie.
Het echotoestel is inclusief het besturingssysteem CE-gemarkeerd. Veiligheidsupdates worden geïnstalleerd nadat ze door de leverancier zijn gevalideerd. Soms betekent dit dat antivirus en security-patches voor het besturingssysteem helemaal niet worden doorgevoerd omdat dit consequenties kan hebben voor de CE-markering. In dat geval zijn dit soort systemen vaak slecht beveiligd tegen invloeden van buitenaf zoals virussen en hacks.

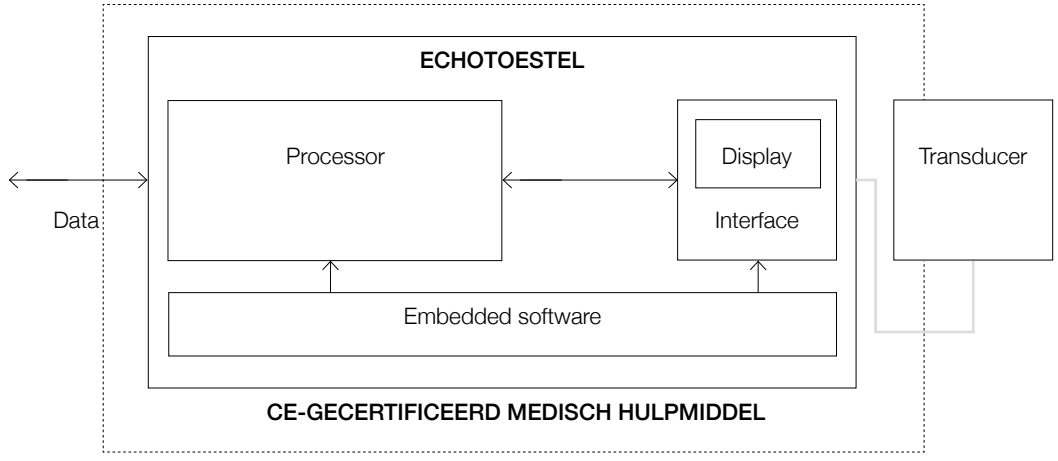
Overwegingen

De apparatuur wordt steeds minder in standalone opzet gebruikt, al kan vaak de eerste diagnostiek gedaan worden via het beeldscherm en de functionaliteiten van

het echotoestel. Echotoestellen worden vaak aan het IT-netwerk van het ziekenhuis verbonden om werklijsten op te halen van het informatiesysteem waarin patiëntafspraken worden bijgehouden, en om beelden te versturen naar een Picture Archiving and Comunication System (PACS).
Als we het echotoestel beschouwen hebben we dus te maken met een medisch apparaat met embedded OS en geïntegreerde software. Dit apparaat wordt vervolgens vaak gekoppeld aan het netwerk terwijl de beveiliging van het apparaat niet altijd up-to-date is.
In deze Praktijkgids richten we ons op de software, de data en de koppelingen aan systemen.
Tijdens de verwervingsfase van een echotoestel moet men in het Pakket van Eisen (PvE) aan een aantal punten zeker aandacht besteden. Eén daarvan is de gewenste koppelingen aan informatiesystemen en het communicatieprotocol dat daarvoor gebruikt moet worden. Ook moet men benoemen hoe omgegaan wordt met de gegenereerde data. Zoals: worden de data lokaal opgeslagen of direct opgestuurd naar het PACS? Hoe lang moeten de gegevens lokaal blijven staan en moeten ze gebufferd worden? Omdat het apparaat vaak aan het ziekenhuis-IT-netwerk gekoppeld wordt, is het van belang dat ook de aansluitvoorwaarden van dit netwerk meegenomen worden in het PvE.
Er zijn diverse mogelijkheden om de echo aan informatiesystemen te koppelen. Dit kan via een dedicated verbinding zijn maar vaak wordt gekozen voor het IT-netwerk van het ziekenhuis dat vervolgens ingedeeld wordt in VLAN's. Via een vast IP-adres of DHCP via het MAC-adres wordt het toestel in het juiste netwerksegment geplaatst. Dit kan voor een bedrade toepassing ook door een netwerkoutlet te koppelen aan het juiste VLAN. Het is afhankelijk van de mogelijkheden van het apparaat (zowel bedraad als draadloos), het standpunt van de leverancier en de voorkeur van de IT-afdeling van de organisatie welke koppelmethode wordt gebruikt.
Er moeten maatregelen genomen worden om een veilige IT-toepassing te garanderen. Dit kan door een up-to-date virusscanner te verlangen van de leverancier. Vaak is dit echter, in verband met de CE-markering, niet toegestaan. Voor de beveiliging kan het echotoestel aan het netwerk worden gekoppeld door deze in een VLAN te plaatsen die achter een firewall met IPS-functionaliteit (Intrusion Prevention System) gesitueerd is. Wel moet men rekening houden met andere bronnen van virussen, zoals het gebruik van usb-sticks. Het risico kan verkleind worden door gebruik van usb-sticks te verbieden en bijvoorbeeld de poorten fysiek af te dichten. Als iemand een usb-stick echt moet gebruiken, bijvoorbeeld tijdens onderhoud van het medische apparaat, dan moet de usb-stick op virussen gescand worden vóór toepassing op het apparaat. Dit kan men vastleggen in de afspraken die met de onderhoudspartij worden gemaakt.

Naast een adequate infrastructuur, en een adequate beveiliging van het apparaat, is het van belang dat wijzigingen aan de software op het apparaat of IT-infrastructuur via een wijzigingsprocedure lopen. Beoordeel eerst of de wijziging wenselijk of noodzakelijk is. Als dat het geval is en de wijziging wordt doorgevoerd, moet het apparaat na de wijziging functioneel getest en vrijgegeven worden. Belangrijk is om ook de koppelingen met informatiesystemen in de testen mee te nemen.
Tijdens diverse stadia van de levenscyclus (bijvoorbeeld voor aanschaf, voor ingebruikname, voor het doorvoeren van wijzigingen) moeten de stakeholders de risico's afwegen.

Casus
Onderstaande tabel beschrijft in samenvatting een voorbeeldaanpak van het echotoestel in figuur 3.1.



Figuur 3.1 Echotoestel

VERWERVINGSFASE	
Wet- en regelgeving	1. Conform de Medical Device Regulation (MDR) of Medical Device Directive (MDD) is het echotoestel, inclusief de embedded software en applicaties die nodig zijn voor een goede werking, CE-gemarkeerd. 2. De IT-netwerk componenten voldoen aan de norm NEN 7510 /ISO 27001 voor informatieveiligheid.
Systeemspecificaties/PvE	1. Het echotoestel, inclusief de embedded software, is CE-gemarkeerd. De leverancier staat alleen gevalideerde updates op het echotoestel toe. 2. Op het echotoestel is geen antivirus software geïnstalleerd. Er zijn andere veiligheidsmaatregelen genomen zoals het plaatsen van het toestel achter een Intrusion Prevention System (IPS). Dit gebeurt in samenwerking met de IT-afdeling van het ziekenhuis. 3. Netwerkcommunicatie vindt plaats op basis van TCP/IP. 4. In het PvE voor aanschaf is opgenomen dat de apparatuur aan informatiesysteem X gekoppeld moet worden. Daarin is de softwareversie van het informatiesysteem X en de informatie die gekoppeld moet worden meegenomen. 5. Voor communicatie wordt gebruikgemaakt van de DICOM-standaard voor modaliteiten. Voor de DICOM-werklijsten dient het IHE-profiel Scheduled Workflow (IHE-SWF) als uitgangspunt.

	6. Het echotoestel voldoet aan de geldende IT-aansluitvoorwaarden. Eventuele afwijkingen (in dit geval het ontbreken van antivirussoftware) zijn besproken met en beoordeeld door de IT-afdeling voor aanschaf van het apparaat. De technische instellingen van het apparaat zijn afgeschermd via een wachtwoord (dit is niet het standaard fabriekswachtwoord).
Security	1. De leverancier van het echotoestel conformeert zich aan het IT-veiligheidsbeleid ten aanzien van de informatiebeveiliging van de patiëntgegevens en neemt preventieve maatregelen tegen virussen en andere dreigingen van buitenaf. 2. Aandachtspunt: vaak gebruikt men één inlog voor alle gebruikers die op het toestel zijn genoteerd, of zelfs geen inlog. Daardoor zijn patiënt-gegevens eenvoudig in te zien. Dit kan bijvoorbeeld opgelost worden door te werken met wachtwoorden of door de fysieke beveiliging van het echotoestel. Security-updates worden vooraf door de leverancier van het echotoestel gevalideerd. Na de update volgt de test- en vrijgaveprocedure die door de medisch technicus, IT'er en de gebruiker wordt uitgevoerd. 3. Omdat het echotoestel geen virusscanner bevat is het gebruik van usb-sticks op deze apparatuur verboden. Een besmette usb-stick kan immers het apparaat en andere apparatuur achter de IPS besmetten. Als iemand een usb-stick moet gebruiken (bijvoorbeeld voor onderhouds-doeleinden), scant de medisch technicus deze eerst op virussen. 4. Conform verplichtingen vanuit de Algemene verordening gegevens-bescherming (AVG) wordt met de leverancier een verwerkersovereenkomst afgesloten volgens het model van de Nederlandse Federatie van Universitair Medische Centra (NFU).
IT-infrastructuur	1. Het echotoestel is opgenomen in het medische VLAN en/of wifi waarvan de toegang wordt bewaakt door een firewall (met IPS-functionaliteit) waarin is gedefinieerd welk dataverkeer tussen het netwerk en het echotoestel mag plaatsvinden. 2. Het opnemen van het echotoestel in het VLAN is door de IT-afdeling gedaan via DHCP, waarvoor een MAC-adres wordt toegevoegd aan het VLAN. Maak afspraken met de IT-afdeling als het opnemen in het netwerk ook in spoedsituaties gedaan moet kunnen worden.
Beheerafspraken	1. De medisch technicus heeft de regie bij het oplossen van storingen en het doorvoeren van wijzigingen. Het technisch beheer van het echotoestel is bij de organisatorische afdeling van de medisch technicus belegd. 2. Er is een WIBAZ/FHI/NEVI Zorg Standaard Service Overeenkomst (SSO) afgesloten met de leverancier. Hierin staan onder andere afspraken over het doorvoeren van updates en upgrades.

GEBRUIKSFASE	
Test- en vrijgaveprocedure	1. De medisch technicus geeft het echotoestel technisch vrij nadat met succes de elektrische veiligheidstest en de voorgeschreven performance-test zijn uitgevoerd. 2. De systeembeheerder/IT'er geeft het systeem vrij nadat de dataverbinding tot stand is gekomen en nadat getest is dat onderzoeken op de juiste plek in het informatiesysteem terechtkomen. 3. De gebruiker geeft het echotoestel klinisch vrij nadat met succes de gebruikersconfiguratie is afgerond en de echo-onderzoeken volgens protocol kunnen worden uitgevoerd. 4. In het configuratiemanagementsysteem van de afdeling Medische Techniek worden ook de software versie en VLAN geregistreerd.
Wijzigingsbeheer	1. Softwarewijzigingen lopen via een wijzigingsproces. 2. Er is een wijzigingscoördinator (in dit geval medisch technicus) aangewezen voor medische apparatuur en alle stakeholders moeten betrokken worden in beoordeling, planning en uitvoering van de wijziging op het echotoestel. 3. Voor goedkeuring van een wijziging worden release notes uitgevraagd. Ook moet de leverancier een vragenlijst invullen met daarop onder andere vragen over de verwachte impact van de wijziging, een planning en een rollbackscenario. 4. Een voorgestelde wijziging wordt aan de hand van een korte risicoanalyse, of bij kleine wijzigingen een risico-inschatting, beoordeeld. 5. Een wijziging wordt eerst op één toestel doorgevoerd en getest. Daarna volgt vrijgave voor gebruik en verdere uitrol over de andere apparaten. 6. De koppelingen van de apparatuur worden meegenomen in de functionele tests. 7. Indien nodig moeten de gebruikers en technici door de wijziging (bijvoorbeeld toevoeging of verandering van functionaliteiten/modaliteiten) een extra instructie krijgen. 8. Ook de periodieke security-updates die door de leverancier worden uitgevoerd, worden volgens de wijzigingsprocedure uitgevoerd. Hiervoor is altijd toestemming nodig van het ziekenhuis (zowel gebruiker, medisch technicus en/of klinisch fysicus, klinisch informaticus als IT'er). Nadat de updates zijn uitgevoerd volgt test- en vrijgaveprocedure.

AFSTOTINGSFASE	
Afstotingsprocedure	1. De patiëntgegevens worden veiliggesteld en moeten van het buiten bedrijf gestelde echotoestel worden verwijderd. Als dit niet mogelijk is, wordt een vernietigingsverklaring opgesteld die de leverancier moet ondertekenen. De softwarelicenties en eventuele onderhoudscontracten worden opgezegd bij buitengebruikstelling.

ERGOMETRIEOPSTELLING

De traditionele 12-kanaals cardiografen die voor de inspanningscardiogrammen werden gebruikt zijn inmiddels vervangen door papierloze digitale systemen. Het inspanningscardiogram wordt nu doorgestuurd naar het elektronisch patiëntendossier. De cardiograaf is vervangen door een werkstation waarop een 10-kanaals-ECG-versterker, ergometerfiets, loopband en een automatische bloeddrukmeter zijn aangesloten. Het werkstation heeft een netwerkverbinding om de werklijsten op te halen en de inspanningsrapportage te versturen. Op het aangesloten scherm wordt het volledige 12-afleidingencardiogram plus ritmestrook weergegeven. Voor de bewaking van de patiënt tijdens de inspanningsoefeningen is dit onmisbaar. De bediening van de aangesloten medische apparatuur vindt ook plaats via het werkstation.

Overwegingen

De eerste overweging bij de aanschaf van dit systeem is de keuze voor een dedicated, door de leverancier geleverde, pc of een door het ziekenhuis beschikbaar gestelde pc. Soms heeft het ziekenhuis hier geen keuze in omdat de CE-certificering alleen geldt bij de geleverde opstelling van de leverancier. In andere gevallen stelt de leverancier eisen aan de door het ziekenhuis te leveren pc. Men kan dan kiezen om bijvoorbeeld de ziekenhuisstandaard in te zetten.

Als het ziekenhuis er samen met de leverancier voor kiest om een dedicated pc van de leverancier te gebruiken, wordt het beheer van de pc bij dezelfde partij belegd als het beheer van de rest van de opstelling. De pc draait dus niet mee in Windows- en antivirussoftware-updates die gecoördineerd worden in het ziekenhuis; dit wordt, altijd pas na validatie van deze updates, geregeld door de leverancier. Vaak zijn deze pc's daardoor niet goed beveiligd waardoor de pc het beste achter een firewall met IPS-functionaliteit kan worden geplaatst als de koppeling aan het netwerk nodig is. Het is dan van belang dat het systeem wel aan de regels voldoet om in dit netwerksegment geplaatst te worden. Zo is vaak geen internetverbinding mogelijk en is het niet toegestaan usb-sticks op de pc te gebruiken. Het voordeel is dat het beheer volledig bij de leverancier ligt en geen andere toepassingen op de pc de werking van het systeem kunnen beïnvloeden.

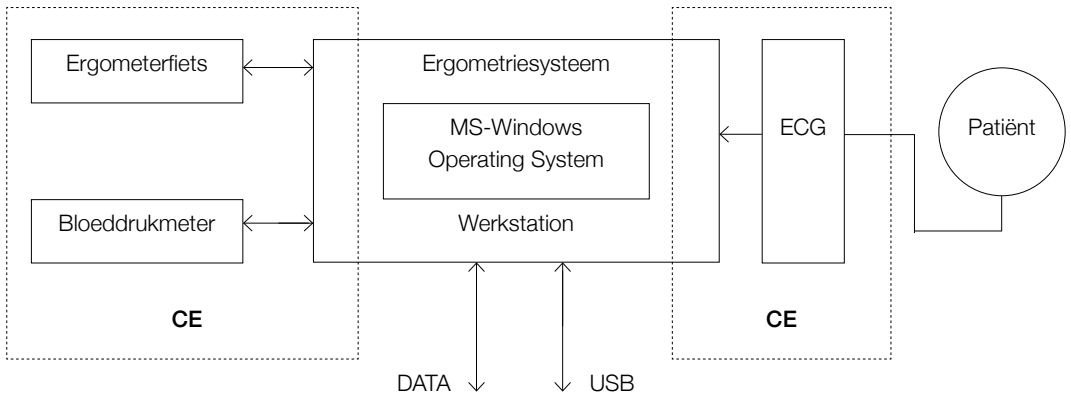
Als een ziekenhuis-pc is gekozen, beheert de IT-afdeling van het ziekenhuis deze pc. Vervolgens moet bepaald worden of deze pc mee kan draaien in de Windows- en antivirussoftware-updates. Als dit het geval is, moeten deze wijzigingen vaak gevalideerd zijn door de leverancier, maar is het ook noodzakelijk dat het ziekenhuis bij elke wijziging de werking controleert. Als dit echter niet het geval is, wordt de pc vaak in een afgescheiden compartiment van het IT-netwerk (achter firewall met IPS-functionaliteit) geplaatst omdat de beveiliging niet gegarandeerd is. In dat laatste geval kan de pc enkel voor die specifieke opstelling worden gebruikt en kan verder geen gebruik worden gemaakt van andere applicaties en internet (of indien nodig enkel op basis van een whitelist met toegestane websites).

Omdat de pc in beide gevallen vaak niet afdoende beveiligd is, moet terughoudend worden gewerkt met usb-sticks zodat deze het apparaat niet kunnen besmetten. De usb-poorten kunnen niet afgeschermd worden omdat de sensoren vaak via usb aan de pc worden aangesloten. Daarom is het belangrijk om de gebruikers duidelijk te instrueren over het verbod om usb-sticks te gebruiken en dit in protocollen vast te leggen. Als iemand toch een usb-stick moet gebruiken, moet de usb-stick eerste gescand worden op virussen op een pc met up-to-date antivirussoftware.

Tijdens de verwervingsfase van een ergometrieopstelling moet men in het Pakket van Eisen (PvE) aan een aantal punten zeker aandacht besteden. Eén daarvan is de gewenste koppelingen aan informatiesystemen en het communicatieprotocol dat daarvoor gebruikt moet worden. Ook moet men benoemen hoe omgegaan wordt met de gegenereerde data. Zoals: worden de data lokaal opgeslagen of direct opgestuurd? Hoe lang moeten de gegevens lokaal blijven staan en moeten ze gebufferd worden? Omdat het apparaat vaak aan het IT-netwerk van het ziekenhuis gekoppeld moet worden, is het van belang dat ook de aansluitvoorwaarden van dit netwerk meegenomen worden in het PvE.

Tijdens diverse stadia van de levenscyclus (bijvoorbeeld voor aanschaf, voor ingebruikname, voor het doorvoeren van wijzigingen) moeten de stakeholders de risico's afwegen.

Casus
Onderstaande tabel beschrijft in samenvatting een voorbeeldaanpak van de ergometrieopstelling in figuur 3.2.



Figuur 3.2 Ergometrieopstelling

VERWERVINGSFASE	
Wet- en regelgeving	1. Conform de Medical Device Regulation (MDR) of Medical Device Directive (MDD) is het ergometriesysteem, inclusief de softwareapplicaties die nodig zijn voor een goede werking, CE-gemarkeerd. 2. De IT-netwerk componenten voldoen aan de norm NEN 7510/ISO 27001 voor de informatiebeveiliging.
Systeemspecificaties/PvE	1. Op het werkstation (door de leverancier geleverde pc) is naast de CE-gemarkeerde softwareapplicaties voor de besturing van de ergometers, monitoring en ECG-registratie ook antivirus- en antimalwaresoftware geïnstalleerd. De leverancier heeft deze software gevalideerd en staat overeenkomstig de onderhoudsvoorwaarden alleen gevalideerde updates op het inspanningssysteem toe. 2. Netwerkcommunicatie vindt plaats op basis van TCP/IP. 3. In het PvE voor aanschaf is opgenomen dat de apparatuur aan informatiesysteem X gekoppeld moet worden. Daarin zijn de softwareversie van informatiesysteem X en de informatie die gekoppeld moet worden meegenomen. 4. Het ergometriesysteem is met de IT-afdeling getoetst aan de geldende IT-aansluitvoorwaarden. Dit is meegenomen in het PvE. Eventuele afwijkingen (in dit geval het ontbreken van antivirussoftware) zijn besproken met en beoordeeld door de IT-afdeling voor aanschaf. 5. De technische instellingen van het apparaat worden afgeschermd via een wachtwoord (dit is niet het standaard fabriekswachtwoord).
Security	1. De leverancier van het ergometriesysteem conformeert zich aan het IT-veiligheidsbeleid ten aanzien van de informatiebeveiliging van de patiëntgegevens en neemt preventieve maatregelen tegen virussen en andere dreigingen van buitenaf. 2. Security-updates moeten vooraf door de leverancier van het ergometriesysteem zijn gevalideerd. De updates worden door de leverancier geïnstalleerd. Na de update volgt de test- en vrijgaveprocedure, die de medisch technicus uitvoert. 3. Het werkstation draait niet mee met de standaard ziekenhuis Windows- en virusupdates. 4. De gebruikers worden geïnstrueerd over het beleid omtrent usb-sticks. usb-sticks mogen niet op de pc worden gebruikt. 5. Conform verplichtingen vanuit de Algemene verordening gegevensbescherming (AVG) wordt met de leverancier een verwerkersovereenkomst afgesloten volgens het model van de Nederlandse Federatie van Universitair Medische Centra (NFU).

IT-infrastructuur	1. De ergometrieapparatuur, ECG-module en automatische bloeddrukmeter zijn op de usb-poorten van het werkstation aangesloten. Voor de ECG-module is ook een draadloze verbinding mogelijk. 2. Het ergometriesysteem is opgenomen in het VLAN waarvan de toegang wordt bewaakt door een firewall waarin wordt gedefinieerd welk dataverkeer tussen het netwerk en het echotoestel mag plaatsvinden. 3. Het opnemen van het ergometriesysteem in het VLAN is gedaan via vast IP-adres. Het IP-adres is daartoe door de IT-afdeling gereserveerd.
Beheerafspraken	1. De medisch technicus heeft de regie bij het oplossen van storingen. Het technisch beheer van het ergometriesysteem is bij de organisatorische afdeling van de medisch technicus belegd. 2. De periodieke security-updates die door de leverancier worden uitgevoerd verlopen volgens een wijzigingsprocedure. Hiervoor is altijd toestemming nodig van het ziekenhuis (zowel gebruiker, medisch technicus als IT'er). Nadat de updates zijn uitgevoerd volgt de test- en vrijgaveprocedure. 3. De functionele wijzigingen aan de software op het apparaat worden ook volgens de wijzigingsprocedure uitgevoerd. 4. Er is een WIBAZ/FHI/NEVI Zorg Standaard Service Overeenkomst (SSO) afgesloten met de leverancier. Hierin staan onder andere afspraken over het doorvoeren van updates en upgrades.

GEBRUIKSFASE

Test- en vrijgaveprocedure	1. Het ergometriesysteem wordt door de medisch technicus technisch vrijgeven nadat met succes de elektrische veiligheidstest en de voorgeschreven performance-test zijn uitgevoerd. 2. De systeembeheerder/IT'er geeft het systeem vrij nadat de dataverbinding tot stand is gekomen en nadat getest is dat onderzoeken op de juiste plek in het informatiesysteem terechtkomen. 3. De gebruiker geeft het ergometriesysteem vrij nadat met succes de gebruikersconfiguratie is afgerond en de inspanningstesten met de fiets of loopband volgens protocol kunnen worden uitgevoerd. 4. In het configuratiemanagementsysteem van de afdeling Medische Techniek worden ook de softwareversie en VLAN geregistreerd.
Wijzigingsbeheer	1. Softwarewijzigingen lopen via een wijzigingsproces. 2. Er is een wijzigingscoördinator (in dit geval medisch technicus) aangewezen voor medische apparatuur en alle stakeholders moeten betrokken worden in beoordeling, planning en uitvoering van de wijziging op het ergometriesysteem. 3. Voor goedkeuring van een wijziging worden release notes uitgevraagd. Ook moet de leverancier een vragenlijst invullen met daarop onder andere vragen over de verwachte impact van de wijziging, een planning en een rollbackscenario. 4. Een voorgestelde wijziging wordt aan de hand van een korte risicoanalyse, of bij kleine wijzigingen een risico-inschatting, beoordeeld. 5. Een wijziging wordt eerst op één toestel doorgevoerd, getest en daarna vrijgegeven voor gebruik en verdere uitrol over de andere apparaten. 6. Indien nodig moeten de gebruikers en technici door de wijziging (bijvoorbeeld toevoeging of verandering van functionaliteiten/modaliteiten) een extra instructie krijgen. 7. De koppelingen van de apparatuur worden meegenomen in de functionele tests.

AFSTOTINGSFASE

Afstotingsprocedure	1. De patiëntgegevens worden veiliggesteld en moeten van het buiten bedrijf gestelde systeem worden verwijderd. Als dit niet mogelijk is, wordt een vernietigingsverklaring opgesteld die de leverancier moet ondertekenen. 2. De softwarelicenties en eventuele onderhoudscontracten worden opgezegd bij buitengebruikstelling.

PACS

Het Picture Archiving and Comunication System (PACS) is software die wordt gebruikt voor de verwerking, bewerking en beoordeling van beelden van verschillende beeldvormende modaliteiten, zoals SPECT, PET, CT en MRI. Maar PACS-software kan ook voor specifieke specialismen worden ingezet. Bijvoorbeeld voor cardiologie, waarbij bewegende beelden van angiografiesystemen en echotoestellen worden opgeslagen als vervanger van de 35-millimeter filmprojector waarmee de hartfilmpjes van de angiografie opnamen werden bekeken. Specialisten beoordelen de beelden op de werk-stations met CE-gemarkeerde diagnostische schermen waarbij de functionaliteiten voor beeldbewerking en berekeningen onderdeel zijn van de PACS-software.

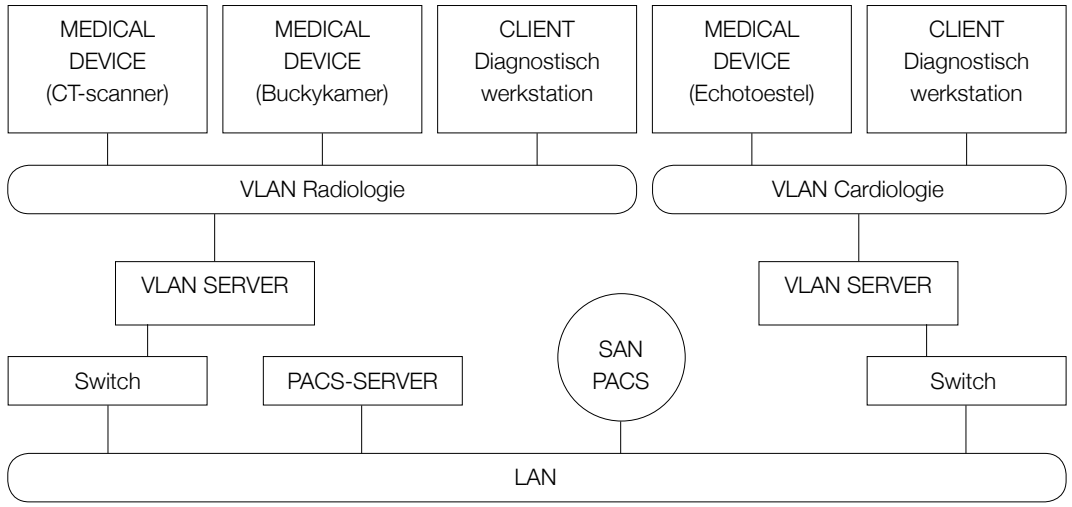
Het PACS is vaak als viewer geïntegreerd in een epd zodat de beelden onderdeel zijn van het dossier van een patiënt. Hierbij worden dan werklijsten voor modaliteiten (indirect) vanuit het epd gegenereerd op basis van de afspraken of orders die voor patiënten worden gemaakt.

Overwegingen

Op de markt is PACS-software in verschillende oplossingen te verkrijgen. Afhankelijk van de intended use van de leverancier wordt PACS-software geclassificeerd als een medisch hulpmiddel. Het kan bedoeld zijn om simpelweg beelden op te slaan en te versturen, dan is het PACS geen medisch hulpmiddel. Als het beeld echter ook bewerkt wordt voor kwaliteitsverbetering of analyse van bijvoorbeeld anatomische structuren voor een

(automatische) diagnose, is er wel sprake van een medisch hulpmiddel. Als PACS-software wordt aangemerkt als medisch hulpmiddel dan moet deze conform Medical Device Directive 2.1/6 ook CE-gemarkeerd zijn.
Ook in de uitvoering kent een PACS verschillende oplossingen. De software kan draaien op een specifiek werkstation, er kan een cloudoplossing gebruikt worden of het kan draaien als client-server applicatie. In alle gevallen is hier sprake van software die via het IT-netwerk is verbonden met beeldvormende modaliteiten en/of andere software. Wanneer de software als een cloudoplossing (of als Software as a Service) wordt aangeboden, vergt dat specifiek op deze situatie gerichte beveiligingsmaatregelen. De leverancier moet zorgen voor een passende IT-infrastructuur en informatiebeveiliging en hij moet in overeenkomsten met afnemers garanties bieden over het op peil houden hiervan.
Daarnaast moet een keuze gemaakt worden voor de inrichting van het beheer. Dit kan centraal worden ingericht of juist decentraal, waarbij eventueel gebruik kan worden gemaakt van key-users.
De opslag van de beelden kan volgens verschillende architecturen worden gerealiseerd: Direct Attached Storage (DAS), waarbij de opslag direct aan slechts één server is verbonden; Network Attached Storage (NAS) en Storage Area Network (SAN) waarbij gebruik wordt gemaakt van netwerkoplossingen.
Als men voor een netwerkoplossing kiest, moeten hiervoor aparte eisen worden opgenomen in het PvE. Ook moeten er eisen worden opgenomen voor de snelheid van de verschillende opslagtypen (hiërarchie): recente beelden moeten sneller beschikbaar zijn dan beelden van een paar jaar geleden.
Er moeten daarnaast functionele eisen worden opgesteld over communicatiestandaarden, standaarden voor opslag en eventuele integratieprofielen. De software moet gebruikt kunnen worden met alle aanwezige merken en modellen beeldvormende modaliteiten, het bestaande ziekenhuisinformatiesysteem en eventueel het bestaande PACS.
Er moeten, gezien het geïntegreerde karakter van de software, uitgebreide integratietesten worden uitgevoerd voordat men het PACS kan gebruiken. Koppelingen met modaliteiten en werklijstbrokers en communicatie met andere software moeten worden getest. Zodra de software in gebruik is genomen mogen toekomstige wijzigingen in de software niet leiden tot beperkingen in functionaliteit. Hiertoe moeten voorafgaand aan wijzigingen impact en risico's in kaart worden gebracht. Tijdens diverse stadia van de levenscyclus (bijvoorbeeld voor verwerving, voor ingebruikname, voor het doorvoeren van wijzigingen) moeten de stakeholders de risico's afwegen.
De bewaartermijn van persoonsgegevens moet in acht worden genomen, waarbij de organisatie zelf verantwoordelijk is voor het bepalen van deze termijn. Identificeerbare persoonsgegevens mogen alleen worden opgeslagen zo lang als nodig voor het doel waarvoor ze dienen. Data kan geanonimiseerd langer worden bewaard, dit geldt ook voor data voor algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Casus
Onderstaande tabel beschrijft in samenvatting een voorbeeldaanpak voor een PACS zoals in figuur 3.3.



Figuur 3.3 PACS-configuratie

VERWERVINGSFASE	
Wet- en regelgeving	1. Het PACS is CE-gemarkeerd conform de Europese Medical Device Regulation (MDR) of Medical Device Directive (MDD). 2. De diagnostische schermen zijn CE-gemarkeerd conform de Europese richtlijn voor medische hulpmiddelen. 3. De IT-netwerkcomponenten die nodig zijn voor een goede werking van software voldoen aan de norm NEN 7510/ISO 27001 voor de informatiebeveiliging.
Systeemspecificaties/PvE	1. Het PACS kan gebruikt worden met alle aanwezige merken en modellen beeldvormende modaliteiten en het bestaande ZIS en PACS. 2. De beelden worden volgens de DICOM-standaard voor modaliteiten opgeslagen en alle DICOM-varianten die in het ziekenhuis worden gebruikt worden ondersteund. 3. Het PACS voldoet aan de eisen voor display-instellingen, weergave van DICOM-velden in het beeld, beeldbewerkingen, beeldenfusie en gebruiksgemak.

	4. De koppeling tussen het ziekenhuisinformatiesysteem en modaliteiten vindt plaats op basis van het HL7-protocol, waarbij het IHE-profiel Scheduled Workflow (IHE-SWF) dient als uitgangspunt. 5. De patiëntgegevens worden in het HL7-ADT-formaat aangeboden. 6. De aangeboden software moet zowel technisch als functioneel kunnen worden getest in een klinische omgeving. Hiervoor moeten performance-eisen opgesteld worden, gericht op het inladen en tonen van beelden en gericht op de samenwerking met andere applicaties zoals spraak-herkenning en verslagleggingssysteem.
IT-infrastructuur	1. Er wordt gekozen voor een client-server oplossing. 2. Een netwerkbroker zorgt ervoor dat de werklijsten in DICOM-formaat naar de modaliteiten worden gestuurd. 3. De door de modaliteiten gegenereerde beelden worden naar de PACS-server gestuurd en opgeslagen in het digitale archief. Er wordt gebruikgemaakt van een SAN-architectuur voor de opslag.
Security	1. De leverancier van het PACS conformeert zich aan het IT-veiligheidsbeleid ten aanzien van de informatiebeveiliging van de patiëntgegevens en neemt preventieve maatregelen tegen virussen en andere dreigingen van buitenaf. 2. Security-updates moeten vooraf door de leverancier van het PACS zijn gevalideerd. De update wordt doorgevoerd met de afgesproken test- en vrijgaveprocedure. 3. Conform verplichtingen vanuit de Algemene verordening gegevens-bescherming (AVG) wordt met de leverancier een verwerkersovereenkomst afgesloten volgens het model van de Nederlandse Federatie van Universitair Medische Centra (NFU).
Beheerafspraken	1. Softwarewijzigingen en storingen worden in het standaard beheerproces van de centrale IT-afdeling opgenomen. 2. Er is een Service Level Agreement afgesloten met de leverancier, met afspraken over onder andere beschikbaarheid, performance, onderhoud en updates. 3. Het applicatie- en serverbeheer van het PACS is belegd bij de centrale IT-afdeling. 4. Het technische beheer voor de diagnostische schermen is belegd bij de medisch technicus of kwaliteitscoördinator. De medisch technicus verricht de kalibratie en kwaliteitsborging volgens zowel voorschriften van de fabrikant als vanuit het veld geldende protocollen, bijvoorbeeld AAPM voor CT [8].

[8] *https://www.aapm.org/pubs/CTProtocols/?tab=5#CTabbedPanels*

GEBRUIKSFASE	
Test- en vrijgaveprocedure	1. Voor functionele en performance-testen van het PACS is een testomgeving volgens de OTAP-methodiek ingericht. 2. In afstemming met andere afdelingen/applicatiebeheerders zijn procedures ingericht om integratietesten uit te kunnen voeren waarbij de juiste werking van communicatie met modaliteiten en interactie/integratie met andere software kan worden vastgesteld. Het PACS wordt door de centrale IT-afdeling op de productieomgeving van de server vrijgegeven nadat met succes de voorgeschreven performance- en integratietesten opgesteld in de verwervingsfase zijn uitgevoerd.
Wijzigingsbeheer	1. Softwarewijzigingen lopen via een standaard wijzigingsproces van de centrale IT-afdeling. Vanuit dit proces worden waar nodig de andere stakeholders tijdig betrokken, bijvoorbeeld Klinische Fysica, Medische Techniek, of applicatiebeheerders van gekoppelde systemen. Een uitgewerkte planning en rollbackscenario worden opgesteld. 2. In de aanloop naar een nieuwe wijziging, worden de release notes opgevraagd om de impact van de implementatie van de nieuwe versie te bepalen. 3. Het applicatiebeheer van gekoppelde softwaresystemen en modaliteiten is belegd bij de betreffende afdeling (kan voor software ook de centrale IT-afdeling zijn). Indien nodig moeten de gebruikers en technici door de wijziging (bijvoorbeeld toevoeging of verandering van functionaliteiten/modaliteiten) een extra instructie krijgen.

AFSTOTINGSFASE	
Afstotingsprocedure	1. De patiëntgegevens worden veiliggesteld en moeten van het buiten bedrijf gestelde systeem worden verwijderd. Let hierbij op eventuele tijdelijke beeldopslag die door de software wordt gebruikt. Als het niet mogelijk is om de data te verwijderen, moet een vernietigingsverklaring worden opgesteld die door de leverancier moet worden getekend. 2. Er moet eventueel conversie van data plaatsvinden om de data in de nieuwe of bestaande IT-omgeving te kunnen bewaren. 3. De softwarelicenties en eventuele onderhoudscontracten moeten opgezegd worden. De bewaartermijn voor persoonsgegevens zoals deze binnen de eigen organisatie vastgesteld is, wordt aangehouden.

TOTAL BODY IRRADIATION SOFTWARE (ZELFBOUW)

Als voorbeeld van zelfbouw standalone software nemen we een applicatie voor de dosisberekening bij Total Body Irradiation (TBI)[9]. Zelfbouw van dit soort applicaties is op radiotherapieafdelingen niet ongewoon.
Bij een TBI-behandeling wordt de gehele patiënt tot een bepaalde dosis bestraald, met uitzondering van enkele organen zoals longen en/of nieren. Omdat bij deze behandeling de gehele patiënt bestraald moet worden, wijkt de geometrie nogal af van de standaardbestralingen waarbij slechts een klein gedeelte van de patiënt (alleen de tumor) wordt bestraald. Daarom is het vaak lastig om met de standaard radiotherapie-planningssystemen de dosisplanning voor deze behandelingen te doen. Voorheen werden tabellenboeken gebruikt om de benodigde machineparameters op te zoeken voor een patiënt. Deze parameters hangen met name af van de doorsnede van de patiënt en de geometrie van de opstelling (zoals de afstand tot de bron). Tegenwoordig zijn deze tabellen vaak vervangen door software die op basis van input de juiste waarden uit tabellen en grafieken haalt en eventueel nog schaalt naar bijvoorbeeld de juiste afstand.

Overwegingen

Als de software alleen dient voor eigen gebruik, wordt degene die de software maakt/levert volgens de Europese Medical Device Regulation niet als leverancier gezien en is CE-certificering niet nodig. Degene die de software ontwikkelt is vrij in de keuze voor de softwareontwikkeltechniek, bijvoorbeeld Scrum, maar moet wel voldoen aan diverse zaken die ook voor externe leveranciers gelden conform de IEC 62304. In deze norm is de levenscyclus voor softwareontwikkeling beschreven. Ook in het geval van wijzigingen aan de software worden aan de ontwikkelaar van de software binnen de eigen organisatie dezelfde vragen gesteld als aan een externe leverancier. We raden daarom ook aan om je als ontwikkelaar te conformeren aan dezelfde verplichtingen die gelden voor een leverancier, waaronder bijvoorbeeld ook het bepalen van de risicoklasse van de software.
De te ontwikkelen software moet worden geclassificeerd als klasse A, B of C conform IEC 62304, afhankelijk van het risico op schade voor de patiënt, gebruiker of enig ander persoon waaraan het falen van de software kan bijdragen. Als er geen risico is op schade aan personen wordt de software geclassificeerd als A. Als er alleen risico is van niet serieuze gezondheidsschade wordt de software geclassificeerd als B. Bij risico op serieuze gezondheidsschade of overlijden van personen wordt de software geclassificeerd als C.
Aan de beslissing tot zelfbouw van een TBI-programma ligt een multidisciplinaire risicoanalyse ten grondslag voor het gebruik van de standaard radiotherapieplanningssoftware voor deze behandeling. De grootste bij deze risicoanalyse gevonden risico's worden met behulp van de zelfgebouwde applicatie afgedekt. Voor de zelfbouwapplicatie zelf moet een risicoanalyse uitgevoerd worden die toegespitst is op de risico's van het gebruik van de applicatie. Denk hierbij aan risico's van foutieve invoer door de gebruiker, het niet up-to-date zijn van meetdata en foutieve extrapolatie van tabellen. Men moet proberen om alle mogelijke situaties in kaart te brengen waarin de applicatie kan falen. Vervolgens moet men deze situaties zo netjes en veilig mogelijk voorkomen. Duidelijke foutmeldingen voor de gebruiker zijn hierbij belangrijk. De bij deze risicoanalyse gevonden risico's moeten worden afgedekt door diverse maatregelen, zoals het inbouwen van extra controles op de invoer, het opnemen van testscenario's in het testplan en opnemen van bepaalde controles in de werkinstructies. Het risicomanagementproces moet gedurende het gehele ontwikkeltraject worden gevolgd.
Software of unknown provenance (SOUP) die wordt gebruikt door de zelfontwikkelde applicatie kan in het geval van software-updates nieuwe risico's introduceren. Voor het TBI-programma worden de berekeningen bijvoorbeeld met een bepaalde versie van Matlab uitgevoerd. In het geval van een nieuwe Matlab-versie moet je als ontwikkelaar nagaan of er nieuwe risico's ontstaan in de berekeningen en of al bekende risico's en maatregelen nog actueel zijn. De risico's van de software en bijbehorende SOUP-versies kunnen in een commercieel beheersysteem, maar bijvoorbeeld ook een Excelwerkblad worden opgeslagen.
Om gebruikers voor de TBI-software te autoriseren moet een keuze gemaakt worden uit de beschikbare mogelijkheden. Er kan bijvoorbeeld een eigen gebruikersdatabase opgezet worden waarin verschillende rollen van gebruikers worden vastgelegd. Maar om aan te sluiten bij al bestaande oplossingen, kan autorisatie verlopen via een standaardprotocol (LDAP/Active Directory). Door deze standaard te gebruiken kunnen gebruikers inloggen met hun netwerk-/werkplek-gebruikersnaam en wachtwoord. De gebruikersnamen en wachtwoorden hoeven hierdoor ook niet binnen de zelfbouwapplicatie opgeslagen te worden, wat ook weer een extra risico zou introduceren. De gebruikersauthenticatie via LDAP is niet zelfgeschreven, maar er wordt een standaardbibliotheek voor gebruikt. Het gebruik van veelgebruikte en goed geteste bibliotheken verkleint de kans op fouten ten opzichte van volledige zelfbouw.
In het ontwerp is gestreefd naar zo min mogelijk afhankelijkheden van andere systemen. In dit voorbeeld van het TBI-programma was dit niet zo moeilijk gezien de geringe complexiteit van het op te lossen probleem. Bij eventuele interactie met andere databases of een PACS moet ervoor worden gezorgd dat de uitgevoerde queries als gevolg van foutieve invoer niet te belastend of schadelijk kunnen zijn voor deze systemen.
Alle data binnen de applicatie worden op het netwerk op gedocumenteerde locaties opgeslagen. Dit voorkomt dat er patiëntgegevens verspreid worden over allerlei computers. Het is bovendien duidelijk welke locaties meegenomen moeten worden in de back-up en ook tijdens de afvoerfase om de data veilig te stellen nadat de software buiten gebruik wordt gesteld.
Bij voorkeur wordt al tijdens het ontwerp en de implementatie rekening gehouden met de eventueel noodzakelijke toegankelijkheid van de data na afvoer van de software. Hiervoor kan bijvoorbeeld het ontwerp modulair worden opgezet (raadpleging los van verwerking) of gekozen worden voor opslag in standaardformaten zoals pdf en DICOM.
De bewaartermijn van persoonsgegevens moet in acht worden genomen, waarbij de organisatie zelf verantwoordelijk is voor het bepalen van deze termijn. Identificeerbare persoonsgegevens mogen alleen worden opgeslagen zolang als nodig voor het doel waarvoor ze dienen. Geanonimiseerde data kunnen langer worden bewaard. Dit geldt ook voor data ten behoeve van algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

[9] *https://en.wikipedia.org/wiki/Total_body_irradiation*

Casus
Onderstaande tabel beschrijft in samenvatting een voorbeeldaanpak voor de TBI-software.

ONTWIKKELINGSFASE	
Wet- en regelgeving	1. Conform de Medical Device Regulation (MDR) is vastgesteld dat er geen commercieel softwarepakket bestaat met de gewenste functionaliteit. 2. De TBI-software berekent hoe een patiënt moet worden bestraald en wordt dus geclassificeerd als klasse C. 3. Er is een softwareontwikkelplan opgesteld met alle op te leveren producten inclusief documentatie en procedures die voor de verschillende fasen van de levenscyclus zijn beschreven. Details hoe een ontwikkelplan op te stellen zijn uitgewerkt in IEC 62304. 4. Het softwareontwikkelplan beschreven in punt 3 wordt gedurende de gehele levensduur van de TBI-software actueel gehouden door de ontwikkelaar. 5. Conform verplichtingen vanuit de Algemene verordening gegevens-bescherming (AVG) worden alleen patiëntgegevens die noodzakelijk zijn vastgelegd en verwerkt in de software. De IT-infrastructuur die nodig is voor een goede werking van de software voldoet aan de norm NEN 7510/ISO 27001 voor de informatiebeveiliging.
Systeemspecificaties/PvE	1. Er is een risicoanalyse uitgevoerd van het bestaande treatment planning systeem die de beslissing tot zelfbouw rechtvaardigt. 2. Risico's uit deze analyse worden afgedekt door de te ontwikkelen TBI-software. 3. Er is een software-requirementanalyse opgesteld conform IEC 62304 en deze is opgenomen in het softwareontwikkelplan en bevat in ieder geval: *a. functionele en niet-functionele eisen;* *b. software-inputs en -outputs;* *c. interfaces met andere systemen;* *d. door software gedreven alarmen, waarschuwingen en berichten voor de gebruiker;* *e. veiligheidseisen (informatiebeveiliging, authenticatie, autorisatie, audit trail, malware beveiliging);* *f. datadefinities en eisen aan de database;* *g. installatie- en acceptatie-eisen;* *h. eisen die worden gesteld aan het gebruik en beheer;* *i. relevante wet- en regelgeving.* De TBI-software moet zowel technisch als functioneel kunnen worden getest in de klinische omgeving.
IT-infrastructuur	1. Er is een software-architectuurontwerp en software gedetailleerd ontwerp conform IEC 62304.
Security	1. De software maakt gebruikt van het LDAP-protocol voor autorisatie van gebruikers via het Active Directory. 2. SOUP-software is gedocumenteerd. Bij updates van deze software of het TBI-programma worden de vooraf in kaart gebrachte risico's getoetst en worden eventuele maatregelen voor nieuwe risico's geïmplementeerd en gedocumenteerd. 3. De ontwikkelaar van de software conformeert zich aan het IT-veiligheidsbeleid ten aanzien van de informatiebeveiliging van de patiëntgegevens en neemt preventieve maatregelen tegen virussen en andere dreigingen van buitenaf. 4. In de ontwikkelomgeving van de software wordt zoveel als mogelijk gewerkt met testpatiënten of fictieve patiëntgegevens.
Beheerafspraken	1. Softwarewijzigingen worden alleen doorgevoerd met de afgesproken test- en vrijgaveprocedure. 2. Er zijn indien nodig afspraken gemaakt met de IT-afdeling van het ziekenhuis over procedures voor softwarewijzigingen, beschikbaarheid van servers, back-up van opslag, etc. Het is raadzaam om uit de WIBAZ/FHI/NEVI Standaard Service Overeenkomst (SSO) de relevante items af te stemmen. 3. Het beheer van servers, database, dataopslag en back-up is belegd bij de IT-afdeling van het ziekenhuis.

GEBRUIKSFASE	
Test- en vrijgaveprocedure	1. Voor functionele en performance-testen van de TBI-software is een testomgeving volgens de OTAP-methodiek ingericht. 2. Alleen de ontwikkelomgeving is afwijkend ten opzichte van niet-zelfontwikkelde software. Programmeurs kunnen eerst verkennende stappen zetten voor wijzigingen aan de software zonder meteen een nieuwe versie te ontwikkelen. Zo kan bijvoorbeeld de juiste werking van de TBI-software met een nieuwe Excelversie worden vastgesteld. 3. Voor de vrijgave van de software is het van belang dat alle testactiviteiten zijn uitgevoerd en de resultaten hiervan bekend zijn. 4. Eventuele afwijkingen die nog in een nieuwe versie zitten, worden beoordeeld op hun risico. 5. Het moet duidelijk zijn welke versie vrij wordt gegeven en de gebruikers moeten weten welke versie gebruikt mag worden.

Wijzigingsbeheer	1. Er is een ontwikkelomgeving volgens de OTAP-methodiek ingericht en er zijn procedures rondom het gebruik hiervan vastgelegd in het software-ontwikkelplan. 2. Softwareconfiguratie en changemanagementprocedures zijn beschreven in het softwareontwikkelplan. De onderdelen die voor het softwarebeheer-proces in IEC 62304 zijn beschreven zijn uitgewerkt: *a. softwareonderhoud, procedures voor correctief onderhoud (bugs) of nieuwe functionaliteit (features);* *b. elke wijziging aan de software moet gekoppeld zijn aan een wijzigingsverzoek;* *c. verkort proces om veranderingen door te voeren bij urgente problemen;* *d. problemen en veiligheidsissues zijn bekend bij de eindgebruiker;* *e. versiebeheer;* *f. regressietesten, waarbij testcases die eerder zijn doorlopen opnieuw worden doorlopen. De huidige uitkomst (na aanpassing) wordt vergeleken met de vorige uitkomst (voor aanpassing). Zo kunnen onbedoelde effecten van de wijziging worden gedetecteerd.* 3. De ontwikkelaar (afdeling) beheert de applicatie functioneel en initieert wijzigingen.

AFSTOTINGSFASE	
Afstotingsprocedure	1. De patiëntgegevens worden veiliggesteld en moeten van het buiten bedrijf gestelde systeem worden verwijderd. 2. Er moet eventueel conversie van data plaatsvinden om de data in de nieuwe of bestaande IT-omgeving te kunnen bewaren. De bewaartermijn voor persoonsgegevens zoals deze binnen de eigen organisatie vastgesteld is, wordt aangehouden.

VOS-MOS-MA

De komende jaren zal de trend in de zorginstellingen doorzetten dat minder zorgprofessionals complexere zorg moeten verlenen. Hiernaast kiezen de zorginstellingen steeds vaker voor éénpersoonskamers vanwege privacy en infectiepreventie. Deze veranderingen hebben veel impact op de observatie en bewaking van de patiënten. Het overzicht over de afdeling wordt moelijker. De technologische ontwikkelingen maken het mogelijk om de alarmen door te sturen naar een draadloze ontvanger/handheld waardoor de observatie niet meer achter de centraalpost hoeft plaats te vinden. De koppeling van het medisch apparaat met een alarmfunctie (bijvoorbeeld fysiologische bewakingsmonitoren) met een oproepsysteem voor de draadloze ontvangers moet voldoen aan de vigerende wetgeving en richtlijnen voor de medische hulpmiddelen en informatiebeveiliging. Het medisch apparaat, de server die de geselecteerde alarmen verzendt en het softwareprogramma in de ontvanger moeten CE-gemarkeerd zijn als medisch hulpmiddel.

We houden hier de volgende terminologie aan:

- VOS: Verpleegkundig Oproepsysteem → patiëntoproepen, assistentoproepen, serviceoproepen en reanimatieoproepen.
- MOS: Medisch Oproepsysteem → medische apparatuur gekoppeld via maak-/breekverbinding aan een alarmsysteem met draagbare devices.
- MA: Medische Alarmeringssysteem → alarmen met context informatie vanuit medische apparatuur worden doorgestuurd naar draagbare devices.

Overwegingen

Voor dit systeem moet men kijken naar de risico's in het gehele systeem en de inzet van het systeem in het zorgproces. Een aantal risico's zijn specifiek van toepassing:

1. onopgemerkt blijven van verstoring ergens in de systeemketen;
2. invloeden van buitenaf zoals hacks, virussen;
3. interferentie van systemen, bijvoorbeeld verstoringen van wifi;
4. afhankelijkheden in de keten (systeem is zo sterk als de zwakste schakel);
5. gebruikersfouten, bijvoorbeeld bij koppelingen;
6. informatie-overload van gebruikers;
7. complexiteit van storingen met mogelijk lange doorlooptijd tot gevolg;
8. infectiegevaar door inzet van niet schone IT-apparatuur in directe zorgomgeving van kwetsbare patiënten, zoals neonaten.

Dit zijn een aantal toprisico's rondom het gebruik van medische oproepsystemen. Het is vooral belangrijk om met elkaar te bespreken wat gedaan moet worden als componenten in de keten niet goed werken. Hoe weet de zorgprofessional dat er een verstoring is in de keten? Welke noodprocedure geldt zodra dit gebeurt? En waar moet de zorgprofessional de verstoring melden?

Een goede en onoverkomelijke basis om de veiligheid van het systeem te borgen, is een uitgebreide multidisciplinaire risicoanalyse voor het medische alarmeringssysteem waarbij alle stakeholders, inclusief gebruikers, betrokken zijn.

Uit risicoanalyses komt direct naar voren dat de keten bestaat uit diverse schakels waarbij de schakels aan de regelgeving moeten voldoen en veilig moeten zijn, maar ook dat de gehele keten als systeem veilig moet zijn. Een dergelijk ketensysteem kan men in zijn geheel laten certificeren door een notified body. Dit kost echter wel veel tijd en geld. Bovendien is het moeilijk om wijzigingen in een ketengecertificeerd systeem door te voeren. Als men niet kiest voor een officieel ketencertificaat moeten het ziekenhuis en de leveranciers wel adequate veiligheidsmaatregelen nemen. Zo is een wijzigingsproces waarin alle stakeholders betrokken worden noodzakelijk. Daarnaast is bijvoorbeeld ketenmonitoring en logging van alarmen belangrijk.

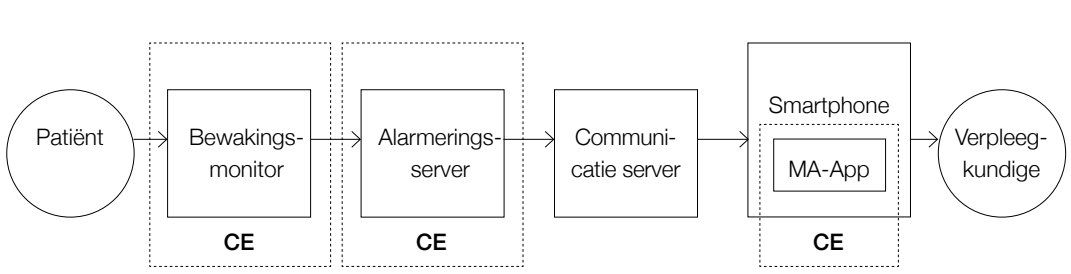
Het wijzigingsproces wordt verder besproken in hoofdstuk 4.8 *Hoe richt ik wijzigingsbeheer in?* Denk bij systemen als medische alarmeringssystemen aan hoe de componenten elkaar beïnvloeden. Zo is het van belang dat onderhoud zoveel mogelijk op elkaar afgestemd wordt zodat het systeem niet keer op keer 'uit de lucht gehaald' wordt. Ook is het van belang dat bij elke wijziging (ook aan de hardware van het IT-netwerk!) gecontroleerd wordt of dit voor de gehele keten zondermeer kan worden doorgevoerd.

Voor elke server moet bekeken en afgewogen worden of deze redundant uitgevoerd wordt, of de server fysiek of virtueel uitgevoerd wordt en of de server voorzien wordt van alle security- en

OS-updates. Als dit laatste het geval is, kan men overwegen de server in een algemeen netwerk te plaatsen. Als de server niet tijdig wordt voorzien van alle security- en OS-updates, moet ook hier een firewall geplaatst worden om de communicatiestromen te reguleren.
Wat betreft beheer is dit een complex systeem. Dit betekent dat alle verantwoordelijkheden expliciet en SMART in een verantwoordelijkhedenmatrix moeten worden benoemd.

De bewaartermijn van persoonsgegevens moet in acht worden genomen, waarbij de organisatie zelf verantwoordelijk is voor het bepalen van deze termijn. Identificeerbare persoonsgegevens mogen alleen worden opgeslagen zo lang als nodig voor het doel waarvoor ze dienen. Geanonimiseerde data kunnen langer worden bewaard. Dit geldt ook voor data ten behoeve van algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Zo kan in dit systeem de anonieme logging van alarmen nuttig zijn voor onderzoek naar trends in alarmering.

Casus
Onderstaande tabel beschrijft in samenvatting een voorbeeldaanpak van de MA in figuur 3.4.



Figuur 3.4 MA

VERWERVINGSFASE	
Wet- en regelgeving	1. Conform de Medical Device Regulation (MDR) of Medical Device Directive (MDD) zijn de berichtenserver die de berichten uit CE-geclassificeerde fysiologische bewakingsmonitor doorstuurt én de software in de draadloze ontvanger CE-gemarkeerd als medisch hulpmiddel. 2. De IT-netwerkcomponenten voldoen aan de norm NEN 7510/ISO 27001 voor de informatiebeveiliging. 3. Het medische apparaat voldoet aan de IEC 60601-1-8. 4. Het ziekenhuis kan de IEC 80001 als handvat gebruiken.
Systeemspecificaties/PvE	1. De koppeling tussen de alarmeringsserver en communicatieserver is door de leverancier van de alarmeringsserver gevalideerd. 2. Op de servers is antivirus- en malwarebeveiligingssoftware geïnstalleerd. 3. De stroomvoorziening voor de alarmeringsserver wordt voorzien van een UPS met voldoende capaciteit als back-up om dataverlies te voorkomen tijdens stroomuitval of andere calamiteiten. 4. Voor de inrichting van de infrastructuur zijn de IT-aansluitvoorwaarden van toepassing, dit is meegenomen in het PvE voor aanschaf. 5. Er is signalering op de draadloze ontvanger bij onderbreking van de verbinding. 6. Er is signalering op de alarmeringsserver bij uitval van de draadloze ontvanger. 7. Er is ketenmonitoring met zichtbare flitslamp op de afdeling die aangaat als ergens in de keten een probleem wordt gedetecteerd. 8. Er is registratie/logging van de alarmen (en de bijbehorende reacties daarop) in de alarmeringsserver, bewakingsmonitoren en op de draadloze ontvanger. 9. Er is een protocol vastgesteld waarin selectie is gemaakt van de noodzakelijk door te sturen alarmen om alarmmoeheid te voorkomen. 10. Er is een OTAP-omgeving ingericht voor dit systeem. Alle voorgenomen wijzigingen kunnen zo eerst in een testomgeving getest worden voordat ze in productie worden doorgevoerd. 11. Als nieuw aan te schaffen medische apparatuur van derden aan het alarmeringssysteem moet worden gekoppeld, wordt de benodigde koppeling met het alarmeringssysteem in het PvE van dit apparaat meegenomen. Daarbij worden dan ook de versienummers van de systemen die gekoppeld moeten worden en de benodigde informatie/ alarmen vermeld. 12. Voor deze nieuw aan te schaffen apparatuur wordt in de verwervingsfase een proof of concept uitgevoerd op de testopstelling om de koppelingen uit te testen.
Security	1. De gebruikers hebben voor uitval van het alarmeringssysteem een noodprocedure opgesteld. 2. Het veiligheidsbeleid van de IT ten aanzien van de cybersecurity is geldend. 3. Conform verplichtingen vanuit de Algemene verordening gegevens-bescherming (AVG) wordt met de leverancier een verwerkersovereenkomst afgesloten volgens het model van de Nederlandse Federatie van Universitair Medische Centra (NFU).
T-infrastructuur	1. De fysiologische bewakingsmonitoren (MH) zijn in een logisch afgescheiden bewakingsnetwerk opgenomen. Dit netwerk bevindt zich achter een firewall met IPS-functionaliteit. Communicatie naar de alarmeringsserver gaat door de firewall waarbij bepaalde poorten in de firewall zijn opengesteld voor dit specifieke verkeer. 2. Er zijn duidelijke afspraken gemaakt over de resources die beschikbaar zijn voor het gehele systeem (geheugen, bandbreedte, hardware). 3. De alarmeringsserver is via VMWare ingericht en zodoende onafhankelijk van verstoringen in de hardware.

	4. De alarmeringsserver is redundant uitgevoerd. 5. De alarmeringsserver staat via het ziekenhuisnetwerk in verbinding met de wifi access points. De netwerkcommunicatie vindt plaats op basis van TCP/IP. De wifi voor de medische berichten is in een VLAN opgenomen en heeft een eigen SSID. 6. Het dekkingsgebied van de wifi is gegarandeerd en afdoende beveiligd, in dit geval via onder andere WPA2. 7. De wifi access points werken via Quality of Service (QoS) waarin de medische alarmen de hoogste prioriteit krijgen.
IBeheerafspraken	1. De medisch technicus heeft de regie bij het oplossen van storingen. Het technisch beheer van de fysiologische bewakingsapparatuur en alarmeringsserver is bij de organisatorische afdeling van de medisch technicus belegd. 2. De medisch technicus heeft bij storingsmeldingen de rol van regisseur tussen de betrokken partijen. 3. De netwerkcomponenten en de wifi zijn belegd bij de organisatorische afdeling van de netwerk- en systeembeheerder. Er zijn duidelijke afspraken gemaakt op gebied van performance en prioriteit. 4. De applicatie van het MA is belegd bij de gebruiker (key-user) van de zorgafdeling. De manager van de betreffende zorgafdeling is de eigenaar van het fysiologische bewakingssysteem en de MA-applicatie. 5. De verantwoordelijkheden zijn expliciet in een verantwoordelijkhedenmatrix beschreven. 6. Er is beleid opgesteld voor het beheer van de handhelds, in dit geval smartphones. Hierin zijn onder andere de levensduur, de Android versie(s) en de softwareversies opgenomen. 7. Er is een onderhoudsovereenkomst afgesloten met alle leveranciers in de keten. De WIBAZ/FHI/NEVI Zorg Standaard Service Overeenkomst (SSO) is daarvoor als basis gebruikt. Dit is verder uitgebreid met bijvoorbeeld een samenwerkingsovereenkomst tussen diverse externe en interne partijen.

GEBRUIKSFASE

Test- en vrijgaveprocedure	1. 1.De ontvangst van de gegeneerde alarmen op de draadloze ontvanger wordt getoetst in het gespecificeerde dekkingsgebied. 2. De signalering op de alarmeringsserver als de ontvanger buiten het dekkingsgebied van de wifi valt, wordt gecheckt. 3. De signalering op de draadloze ontvanger na uitval van het MA wordt gecheckt op de ontvanger. 4. De signalering van de ketenmonitoring op de flitslamp wordt gecheckt.

	5. Het MA wordt door de medisch technicus technisch vrijgeven nadat met succes de elektrische veiligheidstest en de voorgeschreven performance-test zijn uitgevoerd. 6. De systeembeheerder/IT'er geeft het systeem vrij nadat de dataverbinding tot stand is gekomen en nadat getest is dat onderzoeken op de juiste plek in het informatiesysteem terechtkomen. 7. De gebruiker geeft in samenwerking met de klinisch informaticus het MA vrij nadat de gebruikerstest en alle hierboven beschreven testen met succes zijn uitgevoerd. In de configuratiemanagementsystemen van de afdeling Medische Techniek en de IT-afdeling zijn de software versie en VLAN geregistreerd.
Wijzigingsbeheer	1. Er is een coördinator benoemd die alle wijzigingen aan het systeem reguleert en coördineert. 2. De periodieke security-updates die door de systeembeheerder worden uitgevoerd zijn in een procedure vastgelegd. Nadat de updates zijn uitgevoerd volgt test- en vrijgaveprocedure. 3. Wijzigingen en/of vervanging van systeemcomponenten worden met de betrokken beheerders afgestemd op mogelijke consequenties in de functionaliteit en beschikbaarheid voordat de preventieve maatregelen worden uitgevoerd. Tijdens de werkzaamheden is het systeem 'uit de lucht' en kan het niet klinisch gebruikt worden. 4. Wijzigingen worden eerst volledig functioneel getest in de OTA-omgeving voordat ze in de productieomgeving worden doorgevoerd. 5. Nadat de wijzigingen zijn uitgevoerd voert de technisch beheerder de test- en vrijgaveprocedure uit. Het systeem gaat weer 'in de lucht' nadat het door de technisch beheerder is vrijgegeven. 6. Accounts voor individuele medewerkers worden afgesloten als de medewerker uit dienst treedt.

AFSTOTINGSFASE

Afstotingsprocedure	1. De softwareapplicatie wordt verwijderd zodra het MA wordt vervangen door een nieuw systeem. 2. De patiëntgegevens worden door de systeembeheerder veiliggesteld en verwijderd van het opslagmedium. 3. De technisch beheerder zorgt ervoor dat de softwarelicenties en eventuele onderhoudscontracten worden opgezegd. Men houdt zich aan de bewaartermijn voor persoonsgegevens zoals deze binnen de eigen organisatie vastgesteld is (waarbij men rekening houdt met de wettelijke verplichte termijn voor identificeerbare data).

Praktijkvragen

HET ONTWIKKELEN VAN MEDISCHE SOFTWARE/APPS IS EEN VAK WAARBIJ JE ONDER ANDERE ERVAREN ONTWIKKE-LAARS, PROJECTLEIDERS EN ARCHITECTEN NODIG HEBT. HET IS STERK AF TE RADEN ZELF TE ONTWIKKELEN ALS DEZE ERVARING EN KENNIS NIET IN HUIS IS.

4.1 | WAAR MOET IK AAN DENKEN ALS IK ZELF SOFTWARE WIL ONTWIKKELEN?

EUROPESE WETGEVING: MDR EN MDD

In mei 2017 is de nieuwe Europese Medical Device Regulation (MDR) gepubliceerd. Deze vervangt de Medical Devices Directive (MDD). Tot 26 mei 2020 geldt een overgangsperiode waarin leveranciers medische hulpmiddelen mogen laten registreren volgens beide regelingen. Vanaf 26 mei 2020 moeten medische hulpmiddelen voldoen aan de nieuwe regels om toegelaten te worden tot de Europese markt. Hulpmiddelen die vóór 26 mei 2020 gecertificeerd zijn mogen uiterlijk tot 26 mei 2025 op de markt worden gebracht of in gebruik worden genomen.
In de MDD wordt het 'in huis' ontwikkelen van medische hulpmiddelen door zorginstellingen niet expliciet genoemd. Onder deze regelgeving is het dus onduidelijk waaraan zelfontwikkelde software moet voldoen. Dit is anders in de nieuwe MDR. Hierin wordt wel expliciet aandacht besteed aan het 'in huis' ontwikkelen van medische hulpmiddelen door zorginstellingen.
Een zorginstelling heeft tot 26 mei 2020 formeel de mogelijkheid om zelfontwikkelde software in gebruik te nemen die niet aan de eisen van de nieuwe MDR voldoet. Nieuwere versies van deze software, die na deze datum in gebruik genomen worden, zullen echter wel aan deze nieuwe regelgeving moeten voldoen. Meer informatie over wetten, normen en richtlijnen staat in hoofdstuk 4.13. *Wat is de geldende wet- en regelgeving bij medische informatietechnologie?*

'IN HUIS' ONTWIKKELEN: ARTIKEL 5 VAN DE MDR

In het tweede hoofdstuk van de MDR is artikel 5 gewijd aan het op de markt brengen en in gebruik nemen van medische hulpmiddelen. De paragrafen 4 en 5 beschrijven waaraan 'in huis' ontwikkelde medische hulpmiddelen wel en niet moeten voldoen. Met uitzondering van de relevante general safety and performance requirements (GSPR) uit Annex 1 hoeft verder niet aan de in de MDR gestelde eisen voldaan te worden, mits aan een aantal voorwaarden voldaan wordt.
Deze voorwaarden zijn:

a) De medische hulpmiddelen worden niet gedeeld met andere juridische entiteiten.
b) Het ontwikkelen en gebruiken van de hulpmiddelen gebeurt onder geschikte kwaliteitsmanagementsystemen.
c) De zorginstelling rechtvaardigt in de documentatie dat aan de specifieke eisen voor de patiëntendoelgroep niet voldaan wordt door equivalente op de markt verkrijgbare hulpmiddelen.
d) De zorginstelling verschaft op verzoek informatie aan de autoriteiten over het gebruik van dergelijke hulpmiddelen, inclusief een rechtvaardiging voor het ontwikkelen, modificeren en gebruik hiervan.
e) De zorginstelling maakt publiekelijk een verklaring waarin duidelijk staat welke hulpmiddelen 'in huis' ontwikkeld zijn en hoe deze te herkennen zijn. De instelling verklaart ook dat deze hulpmiddelen voldoen aan de relevante general safety and performance requirements (GSPR) uit Annex 1. Als hier niet helemaal aan voldaan wordt, bevat de verklaring een rechtvaardiging hiervoor.
f) De zorginstelling documenteert de structuur van de ontwikkelafdeling, het ontwikkelproces, het ontwerp en de prestaties van de hulpmiddelen, inclusief

het beoogd gebruik. Deze documentatie moet gedetailleerd genoeg zijn om het voor de autoriteiten mogelijk te maken om vast te stellen dat aan de general safety and performance requirements uit Annex 1 wordt voldaan.
g) De zorginstelling zorgt ervoor dat alle hulpmiddelen worden ontwikkeld in overeenstemming met hetgeen onder f) gedocumenteerd is.
h) De zorginstelling evalueert het klinisch gebruik van de hulpmiddelen en neemt indien nodig (correctieve) maatregelen.

ALGEMENE VEILIGHEIDS- EN PRESTATIEVEREISTEN: ANNEX 1 VAN DE MDR

In Annex 1 van de MDR staan de general safety and performance requirements verspreid over 23 paragrafen. Zelfontwikkelde hulpmiddelen moeten aan deze eisen voldoen. Voor software zijn lang niet alle paragrafen relevant, zoals paragrafen met eisen over verpakkingen en transport, sterilisatie of het gebruik van chemicaliën.
De eisen die wel relevant zijn voor zelfontwikkelde software bespreken we hieronder kort. Zoals onder voorwaarde f) hierboven vermeld is, moet de documentatie van de zelfontwikkelde software duidelijk maken dat aan deze eisen wordt voldaan.

Prestaties en veiligheid (GSPR1)
De eerste eis is een algemene eis. Het medisch hulpmiddel moet correct en veilig functioneren en onder normale omstandigheden geschikt zijn voor de intended use.

Risicomanagement (GSPR2 t/m 5, GSPR8)
Deze eisen gaan in op verschillende aspecten van risicomanagement. Risico's moeten geminimaliseerd worden en gewogen tegen de voordelen. Hiervoor moet een systeem voor risicomanagement opgezet worden, waarin dit proces gedocumenteerd wordt. Risicomitigerende maatregelen worden genomen en de gebruikers worden geïnformeerd over eventuele restrisico's. Er wordt ontworpen voor patiëntveiligheid en rekening gehouden met de kennis en ervaring van de gebruikers.

Interactie met de omgeving (GSPR14)
Als een hulpmiddel bedoeld is om te gebruiken in combinatie met andere hulpmiddelen dan moet de hele combinatie veilig zijn. In het ontwerp moeten risico's die voortkomen uit een mogelijke negatieve interactie tussen software en de IT-omgeving waarin deze opereert geminimaliseerd worden.

Elektrisch programmeerbare systemen (GSPR17)
Hulpmiddelen die software bevatten of alleen uit software bestaan moeten zo ontworpen worden dat zij herhaalbaar en betrouwbaar gebruikt kunnen worden voor hun intended use. Een enkele fout, in het systeem of omgeving, mag niet leiden tot gebrekkig functioneren of risico's. Deze situaties moeten netjes afgehandeld worden.
Hulpmiddelen die software bevatten of alleen uit software bestaan moeten ontwikkeld worden op basis van de laatste stand van de techniek op het gebied van ontwikkelprocessen, risicomanagement, informatiebeveiliging, verificatie en validatie.
Als software bedoeld is om gebruikt te worden op mobiele apparaten dan moeten specifieke kenmerken van het apparaat, zoals grootte van het scherm, in het ontwerpproces meegenomen worden.
De ontwikkelaar stelt minimumeisen op voor hardware, IT-netwerken en beveiligingsmaatregelen, die nodig zijn om de software zoals bedoeld te kunnen gebruiken.

GSPR23 Gebruiksaanwijzing
In de gebruiksaanwijzing moet in ieder geval worden opgenomen:
- hoe de software gebruikt moet worden;
- alle zaken die van belang zijn voor een juist functioneren;
- alles wat voor de veiligheid van de gebruiker en anderen van belang kan zijn;
- de hierboven genoemde minimumeisen voor hardware, netwerken, et cetera.

Voor hulpmiddelen in klasse 1 en 2a mag de gebruiksaanwijzing achterwege blijven als deze hulpmiddelen veilig zonder gebruiksaanwijzing te gebruiken zijn.

INTERNATIONALE NORMEN EN HARMONISATIE DOOR DE EU

In het voorgaande werd duidelijk dat de EU eisen stelt als zorginstellingen zelf medische software willen ontwikkelen. Kort samengevat zijn dit eisen op het gebied van:
- kwaliteitsmanagementsysteem;
- risicomanagement;
- ontwikkelprocessen en
- productveiligheid.

Internationale organisaties zoals de ISO (International Organisation for Standardization) en de IEC (International Electrical Commission) hebben over deze onderwerpen de afgelopen jaren normen gepubliceerd, zie tabel 4.1.1. Een aantal van deze normen is door de EU geharmoniseerd. Dit betekent dat wanneer men kan aantonen dat aan deze normen wordt voldaan, verondersteld wordt dat aan de gestelde eisen voor dat specifieke onderwerp wordt voldaan. Geharmoniseerde normen zijn normen die door de Europese Commissie zijn gemandateerd. De betreffende norm krijgt dan de toevoeging EN en in Nederland de toevoeging NEN-EN.
Om een kwaliteitsmanagementsysteem en risicomanagement op te zetten kunnen dus beide door de EU geharmoniseerde normen ISO 13485 en ISO 14971 gebruikt worden.

Organisatie	Norm	Titel	Harmonisatie EU
ISO	13485	Medische hulpmiddelen - Kwaliteitsmanagementsystemen	Ja
ISO	14971	Medische hulpmiddelen - Toepassing van risicomanagement voor medische hulpmiddelen	Ja
IEC	62304	Software voor medische hulpmiddelen - Processen in levenscyclus van programmatuur	Ja
IEC	82304-1	Health Software - Part 1: General requirements for product safety	Nee

Tabel 4.1.1 Internationale normen Medisch Software

Ook IEC 62304 is door de EU geharmoniseerd en deze norm kan dus prima gebruikt worden als blauwdruk voor de op te zetten en te beschrijven ontwikkelprocessen. De IEC 82304-1 norm is pas vrij recent gepubliceerd en nog niet door de EU geharmoniseerd. De verwachting is dat dit in de toekomst wel gaat gebeuren.

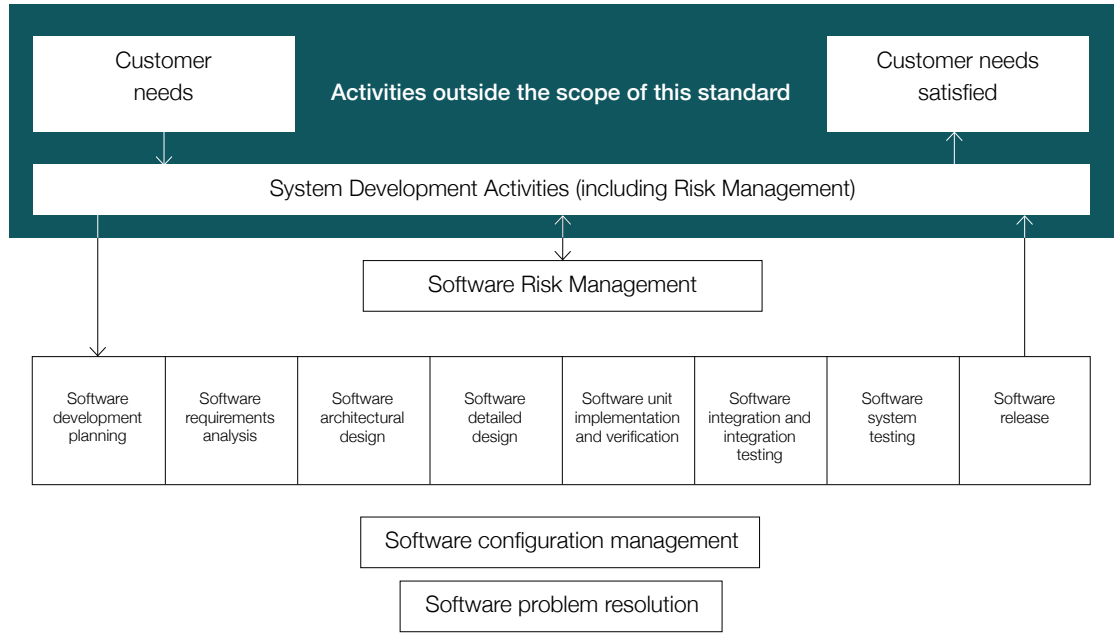
SOFTWAREONTWIKKELPROCES VOLGENS IEC 62304

In de IEC 62304 worden processen voor de levenscyclus van medische software beschreven. Het ontwikkelproces bestaat uit acht processen, zie figuur 4.1.1. Deze processen staan ook vermeld in tabel 4.1.2. Niet alle processen moeten voor alle software doorlopen worden. Het wel of niet verplicht zijn van een proces hangt af van de risicoclassificatie van de software die ontwikkeld wordt.
In IEC 62304 worden drie klassen gehanteerd:

- Klasse A als de software geen schade aan de gezondheid kan veroorzaken.
- Klasse B als de software geringe schade aan de gezondheid kan veroorzaken.
- Klasse C als de software serieuze schade aan de gezondheid of zelfs de dood kan veroorzaken.

Risicomanagement is een integraal onderdeel van IEC 62304. Dit betekent dat in elk proces van de levenscyclus gekeken moet worden of er nieuwe risico's geïdentificeerd kunnen worden op basis van de resultaten van het vorige proces. Voor deze risico's moeten mitigerende maatregelen getroffen worden.

Ontwikkelplan
Het eerste proces van de levenscyclus is het opstellen van een ontwikkelplan. Dit ontwikkelplan beschrijft alle uit te voeren activiteiten en op te leveren producten in de levenscyclus, passend bij de omvang en classificatie van het systeem. Ook configuratieprocedures en changemanagementprocedures worden in het plan beschreven. Dit plan verwijst verder naar de gebruikte ontwikkelingsstandaarden, -methoden en -tools en plannen voor de overige processen. Het ontwikkelplan moet gedurende het hele project actueel gehouden worden.



Figuur 4.1.1 Softwareontwikkelprocessen volgens IEC 62304

Software-requirementanalyse
In dit proces worden de eisen die aan de software worden gesteld gedefinieerd en gedocumenteerd, eventueel op basis van de systeemeisen als de software deel uit maakt van een groter systeem. Hierin worden in ieder geval functionele en niet-functionele eisen meegenomen, evenals in- en uitvoer, interfaces met andere systemen, alarmen, waarschuwingen en berichten voor de gebruiker. Verder is het van belang dat risicomitigerende maatregelen die in software geïmplementeerd moeten worden, opgenomen worden als eis. De requirements moeten duidelijk geformuleerd worden en elkaar niet tegenspreken. Ze moeten eenduidig identificeerbaar, testbaar en tot de bron traceerbaar zijn.

Software-architectuurontwerp
Op basis van de software-requirements wordt in dit proces een software-architectuur ontworpen. Deze architectuur beschrijft de structuur van de software en identificeert de verschillende softwareonderdelen. Daarbij hoort een beschrijving van de interfaces tussen de softwareonderdelen. Als besloten wordt softwareonderdelen te gebruiken van andere komaf (SOUP: Software of Unknown Provenance), dan worden in deze stap de functionele en niet-functionele eisen opgesteld waaraan deze SOUP moet voldoen. Voor systemen in klasse C moet in het kader van risicomanagement in deze fase bekeken worden welke onderdelen gesegregeerd moeten worden. Gesegregeerd betekent in deze context: onafhankelijk van de overige onderdelen, dus bijvoorbeeld draaiend op een eigen processor.

Software detailed design
De software wordt in onderdelen (units) verdeeld. Als het een systeem in klasse C is dan wordt voor al deze units een gedetailleerd ontwerp gemaakt. In deze ontwerpen worden ook de interfaces tussen de units onderling en andere systemen beschreven. Ook moet worden geverifieerd of het gedetailleerd ontwerp de architectuur correct implementeert.

	Klasse		
Proces	**A**	**B**	**C**
Software Development Planning	Ja	Ja	Ja
Software Requirements Analysis	Ja	Ja	Ja
Software Architectural Design	Nee	Ja	Ja
Software Detailed Design	Nee	Nee	Ja
Software Unit Implementation and Verification	Ja	Ja	Ja
Software Integration and Integration Testing	Nee	Ja	Ja
Software System Testing	Ja	Ja	Ja
Software Release	Ja	Ja	Ja

Tabel 4.1.2 IEC 62304 softwareontwikkelprocessen

Software unit implementation
De units worden geprogrammeerd. De validatieprocedure van een enkele unit is afhankelijk van zijn risicoclassificatie. Om een unit samen te voegen met de rest van de code wordt gehandeld volgens het van tevoren opgezette acceptatieplan met bijbehorende criteria. De resultaten van het acceptatieplan worden gedocumenteerd.

Software integration and integration testing
De geïntegreerde software-items worden volgens het integratieplan getest en gedocumenteerd. Met regressietesten, het testen van al aanwezige functionaliteit, wordt aangetoond dat er geen nieuwe problemen zijn. Gecontroleerd wordt onder meer op functionaliteit, afvangen of beheersen van risico's en verkeerd gebruik. De software-integratie- en systeemtesten mogen gecombineerd worden.

Software system testing
Voor het gehele systeem wordt de werking gecontroleerd aan de hand van een verzameling tests, die alle functionaliteiten dekt. Goede uitgangspunten om deze testset samen te stellen zijn de requirements voor het systeem. Voor iedere test wordt de input, verwachte uitkomst, pass/fail criteria, uitvoerend persoon en procedures gedocumenteerd.
De documentatie bevat ook de versie van de software die getest is, evenals relevante hard- en softwareconfiguraties tijdens het testen, gebruikte test tools en de datum van de testen.

Software release
Alvorens de software vrij te geven is het van belang dat men zich ervan verzekert dat alle testactiviteiten zijn uitgevoerd en wat de resultaten hiervan zijn. Eventuele afwijkingen die nog in de versie zitten, worden beoordeeld op hun risico. Het moet duidelijk zijn welke versie vrij wordt gegeven en gebruikers moeten weten welke versie zij mogen gebruiken.

AANDACHTSPUNTEN

Ten slotte nog een aantal zaken die in het voorgaande niet echt aan bod zijn gekomen en specifiek van belang zijn voor zorginstellingen.

Is scripten programmeren?
De Europese wetgeving en ook de internationale normen maken geen onderscheid tussen gebruikte programmeertalen. De gebruikte programmeertaal bepaalt dus niet of er wel of niet aan regelgeving voldaan moet worden. Dit wordt bepaald door de aard van de toepassing. Alleen als een medisch hulpmiddel, met CE-markering, de mogelijkheid biedt functionaliteit aan te passen of toe te voegen via scripts of business logica, en de leverancier staat dit toe voor klinisch gebruik (intended use) kan er beargumenteerd worden dat voor deze scripts of business logica niet apart aan de regelgeving voldaan hoeft te worden. De ontwikkelde scripts of business logica vallen in dit geval onder de originele CE-markering van de fabrikant.
De zorginstelling blijft natuurlijk wel (mede) verantwoordelijk voor veilig gebruik van het medisch hulpmiddel en dus een veilig ontwikkelproces voor deze scripts.

Is configureren programmeren?
Nee, configureren is geen programmeren. Wanneer een leverancier configuratie-mogelijkheden inbouwt voor de eindgebruiker (intended use) moet hij ervoor zorgen dat deze mogelijkheden veilig gebruikt kunnen worden.

Is een Excelsheet software?
De gebruikte programmeertaal bepaalt niet of er wel of niet aan regelgeving voldaan moet worden. Dit wordt bepaald door de aard van de toepassing. Het zou vreemd zijn als een dosisberekening voor Total Body Irradiation geschreven in Excel niet en geschreven in C++ wel aan regelgeving moet voldoen.

Scheiding van rollen
Wanneer in een zorginstelling zelfgeschreven software gebruikt wordt, kan gemakkelijk de situatie ontstaan dat één persoon meerdere rollen heeft, waaronder die van eindgebruiker. Zeker wanneer de persoon die betrokken is bij de ontwikkeling van software, ook de enige gebruiker van deze software is, is het aan te bevelen om een extra persoon te laten toezien op het testen en naleven van de regelgeving.

4.2 | WANNEER MOET IK ZELFONTWIKKELDE MEDISCHE SOFTWARE CERTIFICEREN?

Sommige zorginstellingen ontwikkelen zelf medische apps of medische software omdat dat wat ze zoeken niet op de markt te vinden is of omdat het veel praktischer en goedkoper is om het zelf te ontwikkelen. Er zitten echter nogal wat haken en ogen aan het zelf bouwen en ontwikkelen van medische software en apps. CE-certificering van zelfontwikkelde medische software, en dus ook van een zelfontwikkelde medische app, is vereist wanneer je dergelijke software op de markt wilt brengen. Onder het op de markt brengen wordt ook verstaan het zonder betaling aan een andere partij (lees: andere juridische entiteit) ter beschikking stellen.
Volgens de wet is de 'fabrikant' een natuurlijk persoon of rechtspersoon die een medisch hulpmiddel (lees: ook medische software) ontwerpt en vervaardigt of laat ontwerpen en vervaardigen en het onder zijn eigen naam of merk verhandelt.
In bovenomschreven situatie gaan we ervan uit dat de intended use van deze software, zoals geformuleerd door de fabrikant, valt onder de definitie van een medisch hulpmiddel. De definitie van medisch hulpmiddel kwam in de inleiding al aan bod, maar we herhalen haar hier kort. Een medisch hulpmiddel is:

'elk instrument, toestel of apparaat, elke software of stof of elk ander artikel dat of die alleen of in combinatie wordt gebruikt, met inbegrip van de software die door de fabrikant speciaal is bestemd om te worden gebruikt voor diagnostische en/of therapeutische doeleinden en voor de goede werking ervan benodigd is, door de fabrikant bestemd om bij de mens te worden aangewend voor:

- diagnose, preventie, bewaking, behandeling of verlichting van ziekten;
- diagnose, bewaking, behandeling, verlichting of compensatie van verwondingen of een handicap;
- onderzoek naar of vervanging of wijziging van de anatomie of van een fysiologisch proces;
- beheersing van de bevruchting, waarbij de belangrijkste beoogde werking in of aan het menselijk lichaam niet met farmacologische of immunologische middelen of door metabolisme wordt bereikt, maar wel door dergelijke middelen kan worden ondersteund.'

De in de gezondheidszorg gebruikte 'medische' software kent zeer veel verschijningsvormen. Dit maakt het soms lastig om te beoordelen of bepaalde medische software wel of niet onder de definitie van een medisch hulpmiddel valt. De Europese richtlijn Meddev 2.1.6 is geschreven om deze beoordeling te ondersteunen. Het IMDRF document Standalone Medical Device Software heeft een vergelijkbare functie. Heel algemeen gesteld, en alleen ter indicatie, kun je uit genoemde documenten destilleren dat software die puur dient voor opslag en transport van data op zich geen medisch hulpmiddel is. Zodra er echter sprake is van een bewerking of interpretatie van data gericht op diagnostiek of behandeling gaat het meestal om een medisch hulpmiddel.
Enkele voorbeelden van medische software: software voor planning van radiotherapeutische bestraling, PACS (Picture Archiving and Communication System) met beeldbewerkingsfunctionaliteit, software voor ECG-analyse, software voor digitale pathologie.
Om te bepalen of een hulpmiddel (of specifieke software) wel of niet medisch is volgens de MDD hebben Panton en Netbasics in samenwerking met Syntens een tool ontwikkeld. [10]
Nog meer informatie over medische software is te vinden in de Engelse richtlijn over softwareapplicaties (bijlage III). [11]

Een zorginstelling mag een medisch hulpmiddel in eigen beheer ontwikkelen, bouwen en gebruiken binnen de eigen zorginstelling. De Medical Device Directive stelt hier geen specifieke eisen aan. Uiteraard moet ook daarbij wel aan kwaliteits- en veiligheidseisen worden voldaan. Een zorginstelling is gehouden aan de Wet kwaliteit klachten en geschillen zorg (Wkkgz): '(...) een zorginstelling moet zodanige middelen inzetten dat redelijkerwijs verantwoorde zorg kan worden geboden. Een zorginstelling die zelf medische software ontwikkelt, wordt in het kader van de Richtlijn productaansprakelijkheid (Richtlijn 85/374/EEG) als producent beschouwd en is dan ook aansprakelijk voor eventuele veiligheidsgebreken.'

De Medical Device Regulation (MDR) voor medische hulpmiddelen vervangt de sinds 1993 van kracht zijnde MDD. De MDR is op 26 mei 2017 gepubliceerd en er geldt een overgangstermijn van drie jaar. Voor medische software die is ontwikkeld in de periode tot 26 mei 2020 mag, onder voorwaarden, volgens de MDD worden gehandeld. Daarna moet de MDR worden gevolgd. Zie voor meer informatie en details en uitzonderingsregels ook het hoofdstuk 4.13 *Wat is de geldende wet- en regelgeving bij medische informatietechnologie?*
In de MDR is onder andere een bepaling opgenomen omtrent 'home brew medical devices'. Op grond van deze bepaling mogen zorginstellingen onder de MDR alleen nog zelf medische hulpmiddelen maken als deze hulpmiddelen met de vereiste prestatie niet op de markt verkrijgbaar zijn. Verder moeten de zelfgemaakte medische hulpmiddelen voldoen aan de general safety and performance requirements; afwijkingen daarvan moeten worden onderbouwd. Ook moet het ontwerp adequaat gedocumenteerd worden (technisch dossier), moet de instelling over een passend kwaliteitssysteem beschikken en klinische evaluaties uitvoeren. Feitelijk komt het erop neer dat een in eigen beheer ontwikkeld en gebouwd medisch hulpmiddel praktisch aan dezelfde eisen moet voldoen als waar een externe fabrikant aan is gehouden, minus het aanbrengen van een CE-markering.
De invoering van de MDR kent een overgangstermijn van drie tot vijf jaar (voor IVDR).

IK HEB MEDISCHE SOFTWARE GESCHREVEN, KAN IK DEZE DELEN MET ANDERE ZORGINSTELLINGEN?

Zelfontwikkelde medische software delen met andere zorginstellingen mag enkel als deze voldoet aan de in de MDD of MDR gestelde eisen en voorzien is van een CE-markering. De eisen voor software worden met de komst van de MDR strenger, dit brengt ook extra eisen met zich mee voor een zorginstelling wanneer in eigen beheer ontwikkelde software buiten de eigen zorginstelling wordt gebruikt. Daarnaast valt medische software in de MDR sneller onder klasse 2a/b of zelfs 3 waar software nu volgens MDD nog vaak klasse 1 is.
Een mogelijke oplossing om software beschikbaar te kunnen stellen aan andere ziekenhuizen is om samenwerking te zoeken met een externe fabrikant die wel aan alle gestelde eisen voldoet en dus beschikt over het vereiste kwaliteitssysteem en de nodige kennis en ervaring heeft met risicomanagement, ontwikkeling, testen en validatie van software en met de CE-conformiteitsprocedure. Zij kunnen de software dan verder ontwikkelen, voorzien van een CE-markering en op de markt brengen.

---

[10] *www.cetool.nl*

---

[11] *Zie bijlage III Medical devices software applications including apps op www.mtintegraal.nl.*

MOET IK EEN ZELFONTWIKKELDE APP DIE DOOR MIJN PATIËNTEN WORDT GEBRUIKT VOORZIEN VAN EEN CE-MARKERING?

In eerste instantie is het belangrijk om te na te gaan of deze zelfontwikkelde app ook medische software betreft volgens de definitie van de MDD (tot 26 mei 2020) of de MDR (vanaf 26 mei 2017). De definitie van een medisch hulpmiddel (software) is bij beide normen nagenoeg gelijk. Als de zelfontwikkelde software enkel door eigen patiënten van de zorginstelling en onder begeleiding van de zorginstelling wordt gebruikt, is CE-certificering van deze software niet nodig. Dit moet wel nadrukkelijk goed geborgd worden. Het gebruik van zelfontwikkelde software enkel door eigen patiënten in de thuissituatie wordt gezien als ziekenhuis-verplaatste zorg.
Vóór de ontwikkeling van de software moet wel onderzocht zijn of er geen bestaande alternatieven op de markt zijn met gelijke functionaliteit. Dit onderzoek moet ook gedocumenteerd worden.
Verder moet, volgens de MDR, de zelfgemaakte medische software voldoen aan de general safety and performance requirements; afwijkingen daarvan moeten worden onderbouwd. Ook moet het ontwerp adequaat gedocumenteerd worden en moet de instelling over een passend kwaliteitssysteem beschikken.

IK HEB EEN EXCELBESTAND ONTWIKKELD MET EEN MEDISCHE TOEPASSING. MOET IK DEZE CERTIFICEREN? MAG IK DAT BESTAND DELEN MET ANDERE ZIEKENHUIZEN?

Ook een Excelbestand met een beoogd gebruik dat binnen de definitie van een medische hulpmiddel valt, moet voorzien worden van een CE-markering zodra het bestand gedeeld/verkocht wordt met/aan een andere instelling (andere juridische entiteit). De bouwer van het Excelbestand wordt in dergelijke gevallen gezien als de fabrikant van het hulpmiddel en moet daarom voldoen aan de eisen van de MDD (tot 26 mei 2020) of de MDR (vanaf 26 mei 2017). Zie voor meer informatie en details hoofdstuk 4.13 *Wat is de geldende wet- en regelgeving bij medische informatietechnologie?*

IK HEB MEDISCHE SOFTWARE GEKOCHT VÓÓR 2007, MOET DEZE SOFTWARE VOLDOEN AAN DE MDD OF AAN DE MDR?

Dat software ook een medisch hulpmiddel kan zijn, is in 2007 toegevoegd aan de wetgeving. Een CE-markering is enkel van toepassing op het moment dat het hulpmiddel wordt verkocht aan de zorginstelling. Naast verkoop is dit ook van toepassing bij lening, verhuur, lease of schenking. Medische software vóór 2007 mag gebruikt worden zonder CE-markering. Omdat een instelling is gehouden aan de Wet kwaliteit klachten en geschillen zorg (Wkkgz) moet de instelling er wel voor zorgen dat de software veilig gebruikt kan worden en de risico's bekend zijn.

4.3 | WANNEER MOET IK EEN PROSPECTIEVE RISICO-INVENTARISATIE (PRI) UITVOEREN?

Als antwoord op deze vraag kunnen we stellen: als een toepassing voldoet aan de definitie van een medisch hulpmiddel moet er altijd een prospectieve risico-inventarisatie uitgevoerd worden tijdens de verwervingsfase en tijdens de gebruikersfase (als er sprake is van een wijziging). De mate van detail kan echter variëren.
Dit artikel beschrijft waarom de risico-inventarisatie belangrijk is. Hierbij belichten we zowel de patiëntveiligheid als de bedrijfscontinuïteit. Daarnaast bespreken we methodes om te bepalen in welke gevallen een uitgebreidere risico-inventarisatie zinvol is en in welke gevallen kan worden volstaan met een verkorte risico-inventarisatie.
Het risicomanagement dat we hier beschrijven is van toepassing gedurende de gehele levenscyclus. Tijdens de fasen verwerving en ingebruikname worden risico's vooraf aan het gebruik ingeschat. Dit kan gedaan worden door een prospectieve risico-inventarisatie uit te voeren met beoordeling van risico's op het gebied van patiëntveiligheid. Tijdens de gebruiksfase kunnen door wijzigingen (updates/upgrades) de risico's veranderen. Ook het gebruik in de patiëntenzorg kan veranderen. Dit betekent dat een prospectieve risico-inventarisatie tijdens de gebruiksfase geüpdatet moet worden.
Daarnaast kan er een risico-inventarisatie uitgevoerd worden op de betrouwbaarheid van de patiëntinformatie wat betreft beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Met een business impact analyse (BIA) en een Privacy Impact Analyse (PIA) worden respectievelijk de risico's voor bedrijfsvoering en privacy bekeken.
En juist deze laatste analyse is bijvoorbeeld relevant tot en met de afstotingsfase.

IK MOET EEN PRI OVER EEN BEPAALD SOFTWAREPAKKET UITVOEREN, HOE BEGIN IK?

Om een risico-inventarisatie te maken, staan verschillende methoden ter beschikking zoals SAFER en HFMEA. Deze laatste is door VMS Zorg uitvoerig beschreven in de vorm van een praktijkgids PRI.[12] Daarnaast kan een bow-tie-analyse zinvol zijn. Andere bruikbare bronnen zijn de Leidraad NIKP: nieuwe interventies in de klinische praktijk[13] en het WINT2.0 rapport van de Koepel MT over Risicomanagement ten behoeve van veilig toepassen van medische hulpmiddelen.[14]
In bijlage IV staat een uitgebreid stappenplan PRI, uitgewerkt op basis van het VMS Zorg format.[15]
Een risico-inventarisatie op basis van de HFMEA en SAFER bevat een vijftal stappen, waarbij in stap 4 de daadwerkelijke risico-inventarisatie van het werkproces uitgevoerd wordt.

[12] *https://www.vmszorg.nl/praktijkvoorbeelden-en-tools/herziene-praktijkgids-prospectieve-risico-inventarisatie/*

[13] *Zie bijlage I Leidraad NIKP: nieuwe interventies in de klinische praktijk op www.mtintegraal.nl*

[14] *https://www.wibaz.nl/mdocs-posts/wint-2-0-rapport/*

[15] *Zie bijlage IV Stappenplan uitgebreide prospectieve risico-inventarisatie (PRI) op www.mtintegraal.nl.*

Stap 1 en 2: benoemen PRI en samenstelling projectgroep
In de eerste stap wordt benoemd waar de risico-inventarisatie over gaat. Daarna worden de leden van de projectgroep benoemd. Het is belangrijk dat een multidisciplinaire groep de risico-inventarisatie uitvoert zodat er brede deskundigheid aanwezig is en er vanuit verschillende invalshoeken naar mogelijke risico's wordt gekeken. Welke deskundigen hierbij betrokken moeten worden hangt sterk af van de aard en toepassing en dus van de scope van de analyse: is de software bijvoorbeeld bedoeld voor een specifieke afdeling of voor meerdere afdelingen? De lokaal aanwezige Taken, Bevoegdheden en Verantwoordelijkheden-matrix maakt duidelijk welke stakeholders vertegenwoordigd moeten zijn. Zie ook hoofdstuk 4.4 *Wat verstaan we onder TBV?*
In het geval van medische software, kan gedacht worden aan key-users, klinisch fysicus, klinisch informaticus, medisch technicus, functioneel beheerder, technisch beheerder en IT-architect. Daarnaast moeten deelnemers uit het primaire (zorg)proces, zoals de medisch specialist, verpleegkundige of laborant, vertegenwoordigd zijn.

Stap 3: afbakening
Een PRI gaat nooit over een applicatie of medisch apparaat, maar altijd over het werken met een applicatie. Het is noodzakelijk om het proces goed af te bakenen, passend bij het werkproces, voordat de risico's daadwerkelijk getoetst worden. Dit voorkomt onnodig werk maar ook onnodige discussie in het bestrijden van risico's die functioneel buiten de scope vallen.

Stap 4: analyse van het proces
Voor de beschouwing van het werkproces is het belangrijk om dat proces stapsgewijs te doorlopen, gebaseerd op de mogelijke faalwijzen die kunnen plaatsvinden. Elke faalwijze kent oorzaken en mogelijke gevolgen voor zowel de patiënt en de medewerker als de bedrijfscontinuïteit.
Benoem vervolgens de ernst van de faalwijze en de kans dat deze faalwijze optreedt. Het product van beide is de risicoscore. Bepaal met behulp van een risicomatrix of de vastgestelde risico's acceptabel zijn of niet. In geval van een hoge of zeer hoge risicoscore, moeten er passende tegenmaatregelen benoemd worden.

Frequentie	Enst			
	Catastrofaal	Groot	Matig	Klein
Wekelijks	Zeer hoog	Zeer hoog	Hoog	Laag
Maandelijks	Zeer hoog	Hoog	Laag	Zeer laag
Jaarlijks	Hoog	Laag	Laag	Zeer laag
Minder dan 1x per jaar	Laag	Zeer laag	Zeer laag	Zeer laag

Figuur 4.3.1 Risicomatrix (bron: praktijkgids PRI op www.vmszorg.nl)

Risico's met een hoge risicoscore, moeten worden weggenomen of met een geschikte tegenmaatregel tot een aanvaardbaar niveau worden teruggebracht. Daarna moet nagegaan worden of deze tegenmaatregel geen nieuwe risico's introduceert.

Stap 5: benoemen verbetermaatregel
In stap 4 kunnen tegenmaatregelen benoemd zijn, die nog verdere uitwerking behoeven. Dit zijn de zogenaamde verbetermaatregelen. Deze kunnen van pas komen bij het opstellen van het Pakket van Eisen voor de aanschaf en/of de verdere inrichting van de gebruiksomgeving en de organisatie van het functionele en technische beheer van de software- en IT-infrastructuur. Daarnaast kunnen deze uitkomsten gebruikt worden om de keuzes van het management te verantwoorden over de inzet van geld en middelen. Deze verbetermaatregelen moeten binnen de gestelde termijn opgelost worden.

MOET IK VOOR ALLE MEDISCHE INFORMATIETECHNOLOGIE EEN VOLLEDIGE RISICO-INVENTARISATIE UITVOEREN?

Het is niet zinvol om elk proces zo uitgebreid te analyseren. Een uitgebreide risico-inventarisatie is enkel zinvol als het proces daar om vraagt. Maar hoe bepaal je dit?
Om te bepalen of een zorgproces (met software en afhankelijkheid van IT-componenten) een hoog patiëntveiligheidsrisico heeft, wordt in veel ziekenhuizen een vorm van screening toegepast. Een voorbeeld hiervan is de PRI-screening van het Jeroen Bosch Ziekenhuis (bijlage V).[16] Na het doorlopen van een standaardvragenlijst, wordt op basis van de antwoorden bepaald of een uitgebreide risico-inventarisatie (volgens HFMEA of SAFER) noodzakelijk is.
Voor meer IT-gerichte risico's zijn aparte tools beschikbaar om een eerste risico-inschatting te doen. De BIV, BIA en PIA zijn zo opgezet dat deze een scoring geven als bepaalde belangrijke risico's hoog zijn. Ook hierbij is het mogelijk om een uitgebreidere risico-inventarisatie uit te voeren. Voor een aantal toepassingen zijn al formats of normen beschikbaar. Zo beschrijft de IEC 80001 normenreeks het risicomanagement voor de integratie van medische apparatuur in een IT-netwerk.

[16] *Zie bijlage V PRI-screening Jeroen Bosch Ziekenhuis op www.mtintegraal.nl.*

WAT ZIJN DE VERSCHILLEN TUSSEN PRI, BIV, BIA EN PIA?

Risico's binnen een zorginstelling zijn vanaf meerdere kanten te beschouwen. Om enkel patiëntveiligheidsrisico's te analyseren wordt de PRI gebruikt. Deze methode gaat altijd uit van het risico voor één individuele patiënt. Om risico's te analyseren op het gebied van informatiebeveiliging en bedrijfsvoering zijn respectievelijk de BIV-classificatie (over de betrouwbaarheid van informatie), de BIA (Business Impact Analyse) en de PIA (Privacy Impact Analyse) belangrijk.

BIV-classificatie

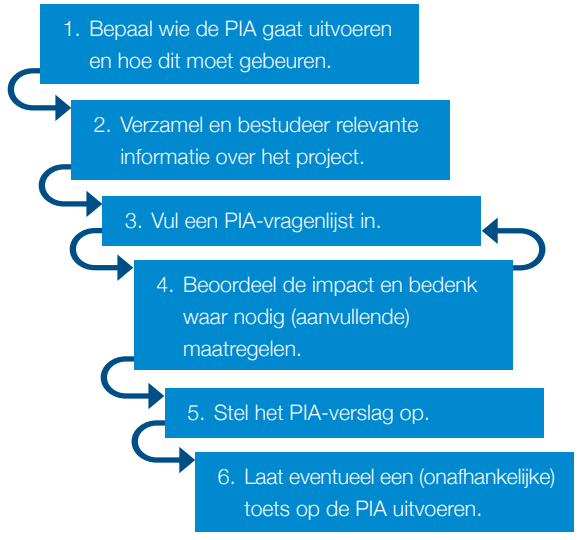
Bij het uitvoeren van een risico-inventarisatie over de betrouwbaarheid van informatie moet men de totale informatietechnologie in ogenschouw nemen, dus ook de hardware en het operating system waarop de software draait en, indien van toepassing, ook de IT-infrastructuur. De uiteindelijke betrouwbaarheid van het informatiesysteem wordt immers bepaald door de betrouwbaarheid van alle onderdelen van het systeem.
De BIV-classificatie geeft een indicatie voor het gewenste beveiligingsniveau van een object. Dat object kan meerdere vormen aannemen zoals informatie of een bedrijfsproces, maar ook een informatiesysteem.
De B staat voor Beschikbaarheid: de mate waarin informatie beschikbaar moet zijn wanneer het bedrijfsproces daar om vraagt. De I staat voor Integriteit: de mate waarin informatie juist, volledig en actueel is en V staat voor Vertrouwelijkheid: de mate waarin informatie alleen toegankelijk is voor daartoe geautoriseerde gebruikers. Een voorbeeld van een BIV-classificatiemethode staat in bijlage VI.[17] Meestal wordt voor de BIV-classificatie een indeling in 3 niveaus gebruikt bijvoorbeeld 3,3,2, wat staat voor: B=3, I=3, V=2. Dit zou bijvoorbeeld de BIV-classificatie voor een epd-systeem kunnen zijn. De BIV-classificatie speelt niet alleen een rol in de verwervingsfase maar ook in de andere fasen van de levenscyclus van medische informatietechnologie. De BIV-classificatie is ontleend aan de norm ISO 27005:2011; Information Technology; Security Techniques; Information Security Management.

BIA

Dit is een risicoanalysemethode waarmee de impact wordt bepaald op de factoren Beschikbaarheid, Integriteit en Vertrouwelijkheid als er storingen zijn in medische informatietechnologie. Wat betreft Beschikbaarheid wordt gekeken naar de business impact wanneer een systeem door een storing een bepaalde tijd niet gebruikt kan worden. Zo kan bijvoorbeeld de vergelijking worden gemaakt tussen de impact van het twee uur uitvallen van een ergometrie-meetopstelling en het epd-systeem. Ook gaat het bij Beschikbaarheid om de impact van het verlies van gegevens.
Bij de BIA wordt gebruikgemaakt van een schaal met vijf niveaus om het impactniveau voor schade te bepalen: catastrofaal, ernstig, belangrijk, gering en verwaarloosbaar. In de analyse wordt aan de hand van een vragenlijst gekeken naar de gevolgen voor verschillende risicogebieden zoals patiënten, medewerkers, verstoring bedrijfsproces, verlieskosten, imagoverlies, aansprakelijkheid en fraude.
De BIA maakt zo duidelijk wat de kritische en minder kritische systemen binnen een zorginstelling zijn. Veelal wordt de uiteindelijke BIA-score omgezet naar een driepuntschaal: laag, midden, hoog. Een voorbeeld van een BIA-vragenlijst is opgenomen in bijlage VII.[18]
De BIA is belangrijk voor de inrichting van de IT-infrastructuur, maar ook om de eisen vast te stellen voor het supportniveau van het functionele en technische beheer. Zo worden de servers en dataopslag van een informatiesysteem met BIA-score 'hoog' zeer waarschijnlijk dubbel uitgevoerd. Ook moeten er goede afspraken en waarborgen zijn voor 24-uursondersteuning, hoge uptime, korte responstijd bij storingen en de inrichting van een volledige teststraat bij het doorvoeren van updates.
De eindverantwoordelijkheid voor de uitvoering en het resultaat van een BIA ligt formeel bij de eigenaar van het proces waarbinnen het systeem gebruikt wordt. De eigenaar beslist over zowel de impact van storingen als over risico's bij wijzigingen in functionaliteit.
De eigenaar is ook verantwoordelijk voor de implementatie en opvolging van de vastgestelde beveiligingsmaatregelen. Beveiligingsmaatregelen kosten tijd en geld en moeten gerechtvaardigd zijn ten opzichte van de te beheersen risico's. Gezien het specialistische karakter worden een BIV en BIA voor de belangrijkere applicaties binnen een zorginstelling veelal het best door een multidisciplinaire groep gemaakt.

PIA

Bij inzet van medische informatietechnologie is het van belang om zorgvuldig om te gaan met de privacy van patiënten en medewerkers. Er worden immers persoonsgegevens vastgelegd en verwerkt waardoor de privacy potentieel risico ondervindt. Een handige tool om privacyrisico's in kaart te brengen, is de Privacy Impact Assessment (PIA). Een geschikte methode hiervoor is die van NOREA, de beroepsorganisatie van IT-auditoren. NOREA raadt aan om de PIA volgens deze stappen uit te voeren:



Figuur 4.3.2 Het stappenplan om een PIA uit te voeren

[17] *Zie bijlage VI BIV-classificatiemethode van Radboudumc op www.mtintegraal.nl.*

[18] *Zie bijlage VII BIA-vragenlijst op www.mtintegraal.nl*

In stap 1 wordt bepaald met wie de PIA moet worden uitgevoerd. Net als voor de andere risico-inventarisaties is het noodzakelijk om de PIA met een team uit te voeren. Vanuit de stakeholdersanalyse kan bepaald worden wie onderdeel moeten uitmaken van het team. Voorbeelden zijn: de opdrachtgever, opdrachtnemer, (toekomstig) gebruiker, expert informatiebeveiliging, expert medische technologie, klinisch informaticus en IT-architect.
Als vervolgens in stap 3 de PIA-vragenlijst wordt ingevuld, gebeurt dit aan de hand van diverse onderwerpen, zoals de gegevens waar het om gaat, de betrokken partijen, de bewaartermijn van de gegevens, de beveiliging en het onderwerp meldplicht datalekken.
Als de vragenlijst is ingevuld, bepaalt de groep de impact, waarbij er onderscheid gemaakt moet worden tussen de impact op de betrokkenen en de impact op de organisatie (imago, financieel). Vanuit de impact kan de groep bepalen waar welke maatregelen geïmplementeerd moeten worden. Meer hierover is terug te vinden in hoofdstuk 4.11 *Wat moet ik doen rondom cybersecurity?*

CONCLUSIE

Een PRI moet altijd uitgevoerd worden als het een informatietechnologie betreft die voldoet aan de definitie van medisch hulpmiddel. Het is echter zinvol te starten met een vorm van screening om te bepalen of een uitgebreidere analyse noodzakelijk is. Deze screening kan zich richten op het patiëntrisico of meer op een continuïteitsrisico voor de patiëntenzorg. Afhankelijk van de uitkomst kan het raadzaam zijn een uitgebreidere analyse uit te voeren volgens bijvoorbeeld het format van VMS Zorg of volgens de formats uit de IEC 80001.
Dit levert vervolgens een PRI op die als levend document gebruikt kan worden gedurende de gehele levenscyclus van de toepassing.

Waar kan ik meer lezen?
Risicomanagement van medische informatietechnologie wordt verplicht gesteld door het Convenant Medische Technologie gedurende de gehele levenscyclus. Vanuit deze richtlijn is meer informatie te vinden. Naast het Convenant bieden de volgende twee richtlijnen ook meer informatie:

- IEC 80001 (IEC 80001-1 Application of risk management for IT networks incorporating medical devices IEC 80001-2-1 Step-by-step risk management of medical IT-networks) en
- IEC 80002-1.

Tot slot wordt vaak aangeraden om risico-management volgens de ISO 14971 uit te voeren.

[19] *Zie bijlage VIII TBV-matrix Amphia Ziekenhuis op www.mtintegraal.nl.*

4.4 | WAT VERSTAAN WE ONDER TBV?

In het convenant, maar ook in verschillende IT-beheermodellen, wordt het belang van het vaststellen van Taken (T), Bevoegdheden (B) en Verantwoordelijkheden (V) beschreven en benadrukt. Hieronder de definities op een rij.

- Taak: een taak is wat iemand **doet** of hoort te doen. Het concrete werk dat iemand verricht, in het licht van zijn verantwoordelijkheid.
- Verantwoordelijkheid: een verantwoordelijkheid is wat iemand **moet.** Diegene is daarop aanspreekbaar en legt daarvoor verantwoording of rekenschap af aan een ander. Verantwoordelijkheid moet niet verward worden met verantwoordelijkheidsgevoel.
- Bevoegdheid: een bevoegdheid is dat wat iemand **mag.** Een bevoegdheid is de toestemming om een bepaalde handeling te verrichten, al dan niet in naam van een ander die deze toestemming gedelegeerd heeft.

WANNEER MOET IK TBV REGELEN/ VASTLEGGEN?

Het is belangrijk dat voor medische informatietechnologie de verantwoordelijkheden voor alle componenten van het systeem voor alle fasen van de levenscyclus zijn vastgesteld en vastgelegd voorafgaand aan de ingebruikname. Dit gaat dan om alle betrokken interne en externe partijen. Hierdoor voorkomt men zoveel mogelijk onduidelijkheden en verschillen in verwachtingen binnen de organisatie tijdens het gebruik.

ENKELE PRAKTIJKVOORBEELDEN UIT ZIEKENHUIZEN

Een praktisch voorbeeld van hoe je dit kunt realiseren betreft een matrix die ziekenhuis-breed betrekking heeft op de gehele levens-cyclus van medische informatietechnologie. In bijlage VIII staat een voorbeeld uit het Amphia ziekenhuis.[19]
In de eerste kolom van de matrix staan de te onderscheiden taken/activiteiten en boven aan de matrix staan alle betrokken partijen. Met een letter in de matrix is aangegeven welke rol welke partij speelt.
De termen RA(S)CI/VERI in dit voorbeeld staan voor:

R (Responsible; **V**erantwoordelijk): degene die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de persoon die accountable is.
A (Accountable; **E**indverantwoordelijk): degene die (eind)verantwoordelijk is en goedkeuring geeft aan het resultaat. Als het erom gaat, moet hij/zij het eindoordeel kunnen vellen, vetorecht hebben. Er is slechts één persoon accountable of eindverantwoordelijk.
S (Supportive; **O**ndersteunend): deze persoon is ondersteunend voor het resultaat. Deze rol lijkt veel op de C-rol.
C (Consulted; ge**R**aadpleegd): deze persoon geeft (mede) richting aan het resultaat, hij/zij wordt voorafgaand aan beslissingen of acties (soms verplicht) geraadpleegd. Dit is tweerichtingscommunicatie. Als RACI gebruikt wordt, is C gelijk aan S.
I (Informed; ge**I**nformeerd): iemand die geïnformeerd wordt over de beslissingen, over de voortgang, over de bereikte resultaten, et cetera. Dit is éénrichtingscommunicatie.

Een tweede voorbeeld betreft een RACI-matrix voor wijzigingsbeheer. Meer over het wijzigingsbeheer staat overigens in hoofdstuk 4.8 *Hoe richt ik wijzigingsbeheer in?*

WIJZIGINGSBEHEER - RACI

R - Responsible (Verantwoordelijk)
A - Accountale (Eindverantwoordelijk)
C - Consulted (Raadplegen)
I - Informed (Informeren)

ACTIE	Projectleider	Projectteam	Programmamanager	Projectondersteuner	Wijzigingsbeheerder	Change Approval Board
1. Registreer de wijziging in logboek	A	I		I	R	
2. Beoordeel de wijzigingsaanvraag	R/A		I	I	C	
3. Informeer de aanvrager over de uitkomst van de beoordeling	R/A	I		C	I	
4. Stuur de wijziging naar Change Approval Board (CAB)	I	I	C	C	R/A	
5. Controleer de wijziging en keur deze goed of af	I		I	C	C	R/A
6. Informeer stakeholders over uitkomst van CAB besluit	C	I		A	R	
7. Herzie projectplannen, risco's indien nodig	R/A	C		A		
8. Update wijzigingslogboek	A	I	I	I	R	I
9. Update programmaplan	C		R/A	I		
10. Implementeer de wijziging	A	R	C	C	I	I

Tabel 4.4.1 Rollen en verantwoordelijkheden in het wijzigingsbeheerproces (bron: www.stakeholdermap.com)

Een derde voorbeeld betreft een TBV-matrix voor een specifiek medisch systeem opgesteld tussen de zorgafdeling, afdeling Medische Techniek, IT-afdeling en de leverancier. In deze matrix (tabel 4.4.2) zijn diverse algemene componenten benoemd met daarbij het eerste en tweede aanspreekpunt.
Het betreft een fietsergometer die aangestuurd en uitgelezen wordt via software op een dedicated pc. Dit is een voorbeeld van algemene afspraken in dit ziekenhuis, maar deze moeten vervolgens vertaald worden naar een specifiek systeem in de projectfase.

	Zorgafdeling	Medische Techniek	IT	Leverancier
Ergometrie fiets/loopband (voldoet als MH)	Eigenaar	Beheer eerste lijn		Beheer tweede lijn
Koppeling (RS-232)	Eigenaar	Beheer eerste lijn		Beheer tweede lijn
Door fabrikant geleverde pc (die voldoet aan de eisen gesteld door leverancier)	Eigenaar		Beheer eerste lijn	Beheer tweede lijn
Software voor aansturing 'Fiets/loopband' op de pc	Eigenaar	Beheer eerste lijn		Beheer tweede lijn
Gevalideerde software voor virusbescherming op de pc	Eigenaar		Beheer eerste lijn	Beheer tweede lijn

Tabel 4.4.2 Voorbeeld TBV

In tabel 4.4.3 hebben we nog een vierde voorbeeld uit een ander Nederlands ziekenhuis opgenomen. Dit is een combinatie van een systeemmatrix met een algemene beschrijving van taken, bevoegdheden en verantwoordelijkheden.

Partijen:	Zorg-afdeling	IT-afdeling	Medische Techniek	Algemene Techniek	Leverancier
Apparatuur:					
Standaardziekenhuis-pc + medische applicatie	E	1			2
Medisch gecertificeerde pc (IEC 60601)	E	1	*		2
PACS-schermen OK-centrum	E	1	*		2
Speciale pc geen onderdeel van medisch apparaat	E	1			2
PDMS pc binnen patiëntengebied	E		1*		2
Smartphone	E	1			2
COW	E	1	*		2
Medische apparatuur (inclusief embedded pc)	E		1*		2
Centraalpost voor bewaking (Drager/Philips)	E		1		2
Lantronix/Digi/EC80 gebruikt voor PDMS	E		1*		2
1-poorts Lantronix/Digi/Moxa niet gebruikt voor PDMS	E	1	*		2
IP Camera	E	1			2
Grabbercard	E	1	*		2
Netwerk		1, E			2
Server		1, E			2
VOS				1, E	2
Niet-ziekenhuisbrede software	1, E				2
Ziekenhuisbrede software		1, E			2

Tabel 4.4.3 Verantwoordelijkheden componenten medische systemen

WAT ZIJN BELANGRIJKSTE AANDACHTSPUNTEN BIJ TBV/VERIMATRICES EN HET BEHEER?

Het is van het grootste belang dat de verantwoordelijken zijn beschreven – voor zowel alle componenten, alsook alle fasen van de levenscyclus van de gehele medische informatietechnologie. Daarnaast moet er aandacht zijn voor de volgende zaken:

- Er moeten afspraken gemaakt worden over alle verschillende vormen van onderhoud. Conform het convenant medische technologie moet het daadwerkelijke onderhoud uitgevoerd worden conform de voorschriften van de fabrikant. Hierop kan alleen onderbouwd afgeweken worden.
- Het proces rondom storingsafhandeling moet zijn ingericht en alle betrokken partijen moeten hun rol daarin kennen en daarvoor ook bekwaam zijn. Denk hierbij ook aan ondersteuning buiten de normale werktijden, zoals een 24-uursondersteuning.
- Ook het changemanagementproces voor de gehele keten van de medische informatietechnologie moet zijn ingericht voor alle componenten van een medisch systeem: apparatuur, software en IT-infrastructuur.
- Voor alle medische informatietechnologie is het van belang dat de taken en verantwoordelijkheden van de verschillende actoren goed zijn beschreven. De actoren voor medische systemen zijn bijvoorbeeld: helpdesk; netwerkbeheer; applicatie- en functioneel beheer; databasebeheer; medische techniek; gebruiker en een externe partij.

WELKE PROBLEMEN KUNNEN ZICH VOORDOEN BIJ EEN NIET GOED INGERICHTE TBV?

- De gebruiker weet niet waar hij met zijn probleem naartoe moet.
- Storingen hebben een lange doorlooptijd omdat niemand zich eigenaar ‘voelt’ van het probleem.
- Het onderhoud van componenten is niet op elkaar afgestemd waardoor het medische systeem meerdere keren voor onderhoud uit de lucht is.
- De impact van changes van componenten van het medische systeem is niet helder waardoor (mogelijk) kritische systemen kunnen uitvallen tijdens gepland onderhoud.

< *Legenda bij tabel links*
1 = Eerste aanspreekpunt, inventariseren probleem, contact met leverancier, tijdens project verantwoordelijk
2 = Oplossen problemen die niet eerstelijns zijn
E = Eigenaar – eindverantwoordelijk – probleemeigenaar
* = Veiligheidskeuring

WELKE VORMEN VAN BEHEER ZIJN ER BIJ IT-AFDELINGEN?

IT-afdelingen hanteren veelal de standaard werkwijzen zoals beschreven in ITIL (Information Technology Infrastructure Library). ITIL beschrijft echter niet de Taken, Verantwoordelijkheden en Bevoegdheden. Men onderscheidt binnen de IT veelal drie vormen van beheer, ook wel beheerdomeinen:

- Technisch beheer. Richt zich op het in stand houden, beheren en onderhouden van de IT-infrastructuur en heeft de Information Technology Infrastructure Library (ITIL) als standaard. De IT-infrastructuur is de basis waarop applicaties kunnen draaien en bestaat uit het netwerk, de computers en operating systems en overige randapparatuur.
- Applicatiebeheer. Onder dit beheer verstaan we het in stand houden van de bedrijfsapplicaties en gegevensverzamelingen van de organisatie. Applicatiebeheer houdt zich bezig met creatie, beheer en wijzigen van applicaties naar aanleiding van geconstateerde fouten of veranderende technische of functionele eisen. De Application Services Library (ASL) is hiervoor binnen IT de standaard. ASL is nieuwer dan en deels geïnspireerd door ITIL.
- Functioneel beheer. Functioneel beheer houdt zich bezig met het beheren van de informatievoorziening in een organisatie. De bedrijfsapplicaties worden gebruikt door de gebruikersorganisatie en moeten eventueel aan veranderende eisen worden aangepast. Het beschrijven van deze wijzigingen, het (laten) doorvoeren van de voorgestelde wijzigingen en het controleren van de wijzigingen behoort tot het takenpakket van Functioneel beheer. Functioneel beheer heeft als standaard Business Information Services Library (BiSL).

Bijlage IX geeft schema's weer die vanuit het IT-landschap als achtergrondinformatie nog een aantal voorbeelden opnemen van de te onderscheiden processen op strategisch, tactisch en operationeel niveau. Omdat dit over het gehele IT-landschap gaat waarbij de medische informatietechnologie een onderdeel is, willen we deze informatie de lezer niet onthouden.[20]

[20] *Zie bijlage IX BiSL model op www.mtintegraal.nl*

[21] *Zie bijlage X Format van een PvE op www.mtintegraal.nl.*

Bij iedere aanschaf van medische informatietechnologie is het noodzakelijk om een Pakket van Eisen (PvE) op te stellen. Met een PvE bereikt men drie doelen. Allereerst zorgt het ervoor dat de eisen en wensen van de diverse betrokken partijen duidelijk zijn en op elkaar afgestemd worden. Daarnaast helpt het PvE om een leveranciersselectie te maken; welke leverancier voldoet het beste aan het opgestelde PvE? Ten derde kan het door de leverancier ingevulde PvE gebruikt worden als onderdeel van het latere koopcontract en een eventuele onderhoudsovereenkomst, waarbij een deel van de afspraken dus al vastligt.

HOE STEL JE EEN PVE OP?

In ieder ziekenhuis moeten de verantwoordelijkheden binnen de levenscyclus van medische hulpmiddelen beschreven en belegd zijn. Hierin is ook aangegeven wie er verantwoordelijk is voor het opstellen van een PvE en wie er betrokken moeten worden. Om een goed PvE op te stellen is er een multidisciplinaire groep nodig. Denk voor de samenstelling van de groep aan de gebruikers en aan de afdelingen Medische Techniek/Klinische Fysica, Klinische Informatica, IT, Inkoop en Hygiëne. Om geen zaken over het hoofd te zien, is het handig om een standaard format voor een PvE te hanteren waarin alle onderdelen benoemd zijn. Alle leden van de multidisciplinaire groep vullen dan het voor hun relevante deel in. De groep moet gezamenlijk de samenhang tussen de diverse eisen en wensen bewaken. Hierbij moeten zij rekening houden met relevante wet- en regelgeving, normen en ziekenhuisbeleid. In bijlage X is een format van een PvE te vinden.[21] Afhankelijk van de structuur van de ziekenhuisorganisatie wordt er uit één van de betrokken afdelingen een projectleider aangewezen om de medische informatietechnologie te verwerven. Deze projectleider moet ervoor zorgen dat de juiste mensen tijdig betrokken worden.

Bij het opstellen van het PvE is het belangrijk om een goede afweging te maken tussen algemene en specifieke eisen. Bij te algemene eisen zullen alle leveranciers voldoen, bij te specifieke eisen kan het voorkomen dat veel leveranciers afvallen. Bij een teveel aan criteria kan het voorkomen dat belangrijke criteria ondersneeuwen door de veelheid aan (minder belangrijke) eisen. Eén van de ontwikkelingen om dit te voorkomen is dat men een functioneel PvE gebruikt. Het ziekenhuis stelt dan de functionele wensen en eisen op papier. Zoals voor welke toepassing is de medische informatietechnologie bedoeld? Op welke afdeling wordt het ingezet? En welke processen moeten ermee ondersteund worden? Dit wordt vervolgens naar de leveranciers gestuurd en die kunnen dan aangeven of en welk product hieraan voldoet. Dit geeft leveranciers meer vrijheid om aan te bieden wat volgens hen bij het ziekenhuis past. Ook nieuwe ontwikkelingen kunnen zo makkelijker meegenomen worden. Informeer bij de afdeling Inkoop wat de gebruikelijke manier van specificeren is binnen het ziekenhuis.

Afhankelijk van de complexiteit van het verwervingstraject kan ervoor gekozen worden om eerst een Request for Information (RFI) op te stellen waarin bij diverse leveranciers informatie opgevraagd wordt om een goed beeld te krijgen van de mogelijkheden op de markt. Op basis daarvan kan dan een Request for Proposal (RFP) opgesteld worden waar het PvE een onderdeel van is. Daarnaast bevat een RFP nog algemene zaken zoals een korte omschrijving van het ziekenhuis en de afdeling waarvoor de medische informatietechnologie bedoeld is, een planning van het verwervingstraject, een gewenste installatiedatum en antwoordinstructies.

Naast dat het PvE in een multidisciplinair team wordt opgesteld is het ook van belang om de antwoorden van de leveranciers in een multidisciplinair team te beoordelen.

WAT MOET ER IN HET PAKKET VAN EISEN STAAN?

Hieronder noemen we de belangrijkste eisen/vragen/aandachtspunten die in een PvE moeten staan. In hoofdstuk 3 *Praktijkvoorbeelden* staan per type medische informatietechnologie voorbeeldeisen genoemd.

- Welke eisen stelt de leverancier aan de verschillende type systemen waar de software op moet kunnen draaien: op welk besturingssysteem, binnen welke architectuur, et cetera?
- Software-updates: hoe vaak, kosten, verantwoordelijkheden, hoe lang na aanschaf?
- Softwarelicenties: aantal gebruikers, type licentie, eigendom.
- Remote beschikbaarheid van applicatie-software.
- Hoe vindt de software-installatie plaats: wel of niet via het netwerk?
- Welke serversoftware wordt er gebruikt of is er vereist?
- Hoe garandeert de leverancier database-compatibiliteit?
- Hoe vindt communicatie met andere systemen plaats, zoals gebruik van DICOM of HL7?
    - Denk hierbij specifiek aan het vermelden van de versienummers van de systemen waaraan gekoppeld moet worden (bijvoorbeeld Metavision PDMS versie 5.xx). Dit voorkomt het probleem dat een koppeling wel goed werkt met een bepaalde versie software terwijl deze versie (nog) niet in de zorginstelling in gebruik is.
    - Denk hierbij ook aan de informatie die je via een koppeling wilt uitwisselen, zoals alarmen of data. Als er cruciale alarmen in de koppeling moeten worden doorgegeven specificeer dan vooraf welke en op welke manier.
    - Denk eraan dat de vraag of iets gekoppeld kan worden nog niet betekent dat de koppeling al beschikbaar is vanuit beide partijen. Wees concreet en geef aan dat op een bepaalde datum de driver voor de koppeling werkend beschikbaar moet zijn. Bedenk hierbij ook wie dat betaalt, en dat het juiste communicatieprotocol gebruikt wordt.
- Wat levert de leverancier aan antivirus-software, malwaredetectie/-preventie en hoe houdt de leverancier dit up-to-date? Kan de antivirussoftware van het ziekenhuis gebruikt worden? Zo ja, welke eisen stelt de leverancier hieraan?
- Welke hoeveelheid data dient opgeslagen te worden?
- Data moeten zoveel mogelijk centraal opgeslagen worden. Hoe wordt dit geregeld, welke koppelingen zijn hiervoor nodig? Worden er nog data lokaal opgeslagen? Zo ja, hoe lang/hoeveel?
- In welk dataformaat wordt de data opgeslagen (bijvoorbeeld DICOM), en hoe garandeert de leverancier toekomst-bestendigheid hiervan?
- Datadefinitie: volgens welke systematiek moeten de gegevens vastgelegd worden? Denk aan 11-cijferige patiëntennummers of specifieke eisen vanuit EZIS.
- Wat heeft de leverancier geregeld voor back-ups, dataverlies bij stroomuitval of andere calamiteiten en het loggen van foutmeldingen?
- Wat heeft de leverancier geregeld voor (patiënt-)databeveiliging (denk ook aan privacy, autorisatie, uitwisseling van gegevens) en wat moet het ziekenhuis hier zelf voor regelen?
- Biedt de leverancier de mogelijkheid van conversie van oude data?
- Is het mogelijk om aanpassingen in de applicatie door de eindgebruiker en/of ziekenhuis-IT te laten aanbrengen? Bijvoorbeeld het zelf opstellen van scripts om databases, back-ups en dergelijke aan te maken.
- Welke mogelijkheden biedt het systeem om een rechtenstructuur in te richten? Denk aan creëren, lezen, wijzigen en verwijderen van data (rechten, bewaartermijnen, mogelijk ook rechten voor patiënt, audit trail).
- De software in het medisch apparaat moet onderdeel zijn van de CE-certificering van het medische apparaat. Als het gaat om standalone medische software moet deze zelfstandig CE-gemarkeerd zijn.
- IT-aansluitvoorwaarden/infrastructuureisen voor apparatuur/software op het netwerk als dit van toepassing is voor de zorg-instelling. In deze aansluitvoorwaarden staan veelal zaken als: DHCP, AD, DNS, geen fixed IP-adres, up-to-date zijnde OS en antivirus.

AFWEGINGEN

Afhankelijk van het type medische informatietechnologie moet men soms kiezen tussen ziekenhuisstandaarden of leveranciersspecifieke oplossingen. Denk hierbij aan een dedicated pc of een ziekenhuis-pc, antivirussoftware die ziekenhuisbreed gebruikt wordt of leveranciersspecifieke software en een dedicated netwerk of het ziekenhuisnetwerk. Vanuit beheeroogpunt is het meestal wenselijk om voor de ziekenhuisstandaard te kiezen, maar niet alle leveranciers werken hieraan mee. Het is daarom van belang om dit goed uit te vragen bij de leverancier. Is het mogelijk om voor de ziekenhuisstandaard te kiezen, en zo ja, welke eisen stelt de leverancier dan en welke inspanning leveren zij om het ziekenhuis hierbij te ondersteunen? Goede afspraken tussen leverancier en ziekenhuis over bijvoorbeeld verantwoordelijkheden en aansprakelijkheden zijn hierbij noodzakelijk. Zie voor verdere informatie hierover hoofdstuk 4.9 *Welke beheerafspraken moet ik maken met welke partijen?*

4.6 | WAT IS EEN OTAP EN WAT IS HET NUT DAARVAN?

Voordat de medische informatietechnologie in gebruik kan worden genomen moet de gehele medische informatietechnologie getest en gevalideerd worden. Hiervoor wordt vaak een OTAP-omgeving ingericht. Dit acroniem staat voor:

- Ontwikkelomgeving (meestal alleen bij de fabrikant)
- Testomgeving (onderdeel van de initiële installatie)
- Acceptatieomgeving (een recente kopie van de Productieomgeving inclusief de koppelingen)
- Productieomgeving (de uiteindelijke productieomgeving)

Het accent van de testen ligt vooral op het controleren van een goede werking van de software, het goed functioneren van alle koppelingen en interfaces en het correct bewerken en verwerken van de aangeboden data in de bijbehorende workflow van de zorginstelling.
Wanneer het gehele systeem correct functioneert en aan de overige randvoorwaarden is voldaan, kan de medische informatietechnologie klinisch in gebruik worden genomen.

WAT HEB IK VOOR EEN OTAP NODIG?

Voor validatie/verificatie van medische informatietechnologie (inclusief de keten) is het noodzakelijk om naast de productie- (klinisch gebruik) ook een acceptatieomgeving beschikbaar te hebben. Hierbij is het belangrijk dat de acceptatieomgeving een representatieve omgeving is. Denk hierbij aan de gehele keten tijdens het klinisch gebruik, en bij databases bijvoorbeeld aan de load voor realistische performance-testen (regressietesten).
Hierbij moet dus ook gedacht worden aan de gekoppelde randapparatuur en/of in- en externe datakoppelingen. Om een OTAP in te richten is ook een beschrijving van het technisch en functioneel ontwerp noodzakelijk, zoals de aanwezige technische koppelingen en interfaces. IT-architecten vertalen het technisch en functioneel ontwerp in een zogenaamde architectuurplaat. Hierop zijn alle onderlinge afhankelijkheden zichtbaar gemaakt.

WAT ZIJN AANDACHTSPUNTEN BIJ EEN OTAP-INRICHTING?

De verschillende O-,T-, A- en P-omgevingen zijn virtueel dan wel fysiek van elkaar gescheiden. De praktische invulling van een OTAP-omgeving kan van diverse factoren afhankelijk zijn, zoals de complexiteit van de te beoordelen softwareapplicaties en de complexiteit en inrichting van de eigen organisatie. Er moeten minimaal een A- en P-omgeving zijn.
Relevante informatie en tools die helpen om een OTAP-omgeving op te zetten zijn bijvoorbeeld:

- ITIL-processen;
- ANTILOPE - Adoption and take up of standards and profiles for eHealth Interoperability;
- IHE Connectathon/DICOM.[22]

Voor deze koppelingen moeten mogelijk op basis van de praktische uitvoerbaarheid en de inrichting van de infrastructuur specifieke keuzes worden gemaakt. Kun je bijvoorbeeld de functionele of gebruikerstesten in een acceptatieomgeving overal in de organisatie uitvoeren of alleen op specifieke werkstations (zijn deze representatief voor productie)? Of zijn er afhankelijkheden met het netwerk door IP-filteringen waardoor er een verschil met de uiteindelijke productieomgeving is? Voor het netwerk wordt voor medische toepassing veelal een VLAN gecreëerd – een virtueel gescheiden netwerk.

[22] *https://www.ihe-nl.org/ihe-deelnemers/tieto-netherlands-healthcare-bv*

PRAKTISCHE UITDAGINGEN BIJ EEN OTAP

Het is in de praktijk niet altijd eenvoudig om een OTAP in te richten. Hieronder geven we een aantal voorbeelden van praktische uitdagingen.

- Bij koppelingen in zijn algemeenheid bijvoorbeeld met ADT is het belangrijk te borgen dat er geen naar echte patiënten herleidbare productiedata in de OTA-omgevingen beschikbaar of zichtbaar zijn.
- Een Patiënt Data Management Systeem (PDMS) waarbij via een specifieke gateway de HL7-verstuurde vitale parameters in het PDMS-systeem komen. Als verantwoordelijke organisatie zou men afhankelijk van de geïnventariseerde risico's voor de acceptatie op basis van de productieomgeving een 'mini' patiëntmonitoringsysteem (bedzijdige patiëntbewakingsmonitor en centraal post) en een HL7-gateway kunnen inrichten.
Dit geeft mogelijk naast financiële uitdagingen, gezien het fysiek scheiden van de omgevingen, ook netwerkarchitectuur-technische uitdagingen. Een oplossing kan hierbij het werken met virtuele netwerken en domeinen zijn.
- Een update van een Medisch Oproep Systeem (MOS-) en/of Medisch Alarm (MA-) keten.
Hierbij kan het – afhankelijk van de aanwezige infrastructuur en de gebruikte devices, zoals oproep-pagers – lastig zijn een representatieve test- en acceptatieomgeving te maken. Bijvoorbeeld vanwege kosten of hoge infrastructuureisen. Voor de oproep-pagers is naast een IT-oplossing via wifi ook veelal een specifieke infrastructuur met HF-zenders aanwezig. Omdat het om primaire alarmeringsvoorzieningen gaat is het testen en accepteren een heel belangrijk onderdeel van het validatieproces. Om toch te kunnen valideren kan een oplossing zijn om het systeem in de productieomgeving te testen of om het systeem gefaseerd (afdeling voor afdeling) over te zetten naar een nieuwe softwareversie. Ook kan het een optie zijn om in overleg met de zorgafdeling het MOS/MA gedurende een afgesproken tijd uit de lucht te halen om alle benodigde werkzaamheden uit te voeren. De afdeling kan zich dan voorbereiden door maatregelen te treffen, zoals het permanent bezetten van de centrale post met de centrale bewakingsmonitoren.
- Aanpassing in het TBI-dosisberekeningsprogramma. Hierbij is alleen de ontwikkelomgeving afwijkend ten opzichte van de situatie met niet-zelfontwikkelde software. In deze omgeving kunnen programmeurs de eerste verkennende stappen zetten om de software te wijzigen, zonder meteen een geheel nieuwe versie te bouwen. Als er bijvoorbeeld berekeningen in Excel worden gedaan, kan experimenteel worden bekeken of de software ook werkt met een nieuwe versie van Excel. Indien nodig kan men dan enkele wijzigingen in de eigen software programmeren. Zie ook hoofdstuk 4.8 *Hoe richt ik wijzigingsbeheer in?* bij de fase gebruik.
- Validatie van een virusscan. De OTAP-omgeving wordt gebruikt om te testen in hoeverre een kritische update om virussen te voorkomen invloed heeft op de softwareapplicatie. Veelal worden deze virusscans als kritische update beschikbaar gesteld, het is belangrijk om samen met de fabrikant afspraken te maken over het doorvoeren van deze updates.

Een aantal van deze aandachtspunten is in de WIBAZ/FHI/NEVI Zorg SSO [23] opgenomen, het advies is om deze te hanteren.

[23] *https://www.wibaz.nl/mdocs-posts*

HOE KAN IK MIJN OTAP UP-TO-DATE EN REPRESENTATIEF HOUDEN?

Bij de inrichting van een OTAP is het representatief houden van de verschillende OTAP-omgevingen noodzakelijk. Dit kan bijvoorbeeld door het up-to-date houden van de configuratiemanagementdatabase (CMDB). Idealiter wordt in een CMDB alle beschikbare informatie opgeslagen: pc's, werkstations, servers, applicaties, licenties, gebruikers, et cetera.
Met zo'n database kunnen allerlei relaties worden gelegd en is te zien welke applicaties gebruikmaken van welke servers en databases, wie de gebruikers zijn en wie de beheerders zijn. Zowel bij het oplossen van storingen als het doorvoeren van wijzigingen is dergelijke informatie van groot belang.
Bij wijzigingen in de CMDB kan er een check plaatsvinden of er een impact met de OTAP-omgevingen is. Dit kunnen naast hardware- ook softwareversies zijn.
Het is dan ook cruciaal dat alle betrokken partijen toegang hebben tot de informatie in de CMDB en zich verantwoordelijk voelen om alle informatie in deze database gedurende de gehele levenscyclus van de medische informatietechnologie up-to-date te houden.

4.7 | HOE KAN IK MEDISCHE APPARATUUR VEILIG KOPPELEN AAN HET IT-NETWERK?

Medische apparatuur wordt in toenemende mate gekoppeld aan het IT-netwerk van het ziekenhuis. Dit brengt voor- en nadelen met zich mee. Door de toenemende afhankelijkheid van het IT-netwerk voor de juiste werking van medische apparatuur is het belangrijk dat de juiste aandacht wordt gegeven bij de inrichting van het netwerk. Een voorbeeld waarbij een medisch apparaat sterk afhankelijk is van het netwerk om optimaal te kunnen functioneren is een hartbewakingsmonitor die in connectie staat met de centrale post. De monitor kan standalone werken, maar de optimale werking wordt bereikt als de connectie via het netwerk met een centrale post optimaal functioneert. Medische apparatuur kan op meer dan één manier aan het IT-netwerk gekoppeld worden en de situatie verschilt per ziekenhuis. Het is wel belangrijk om bij een dergelijk proces de juiste deskundige te betrekken en de relevante normen en procedures te kennen. Houd rekening met de volgende disciplines bij configuratie van het netwerk voor medische apparatuur:

- IT-architect;
- IT-netwerkbeheer;
- medisch instrumentatietechnicus;
- verpleegkundige/hoofd betrokken zorgafdelingen;
- klinisch informaticus en/of klinisch fysicus en/of biomedisch technoloog.

Naast de technische inrichting is het belangrijk om de procedures en verantwoordelijkheden goed te hebben ingericht, omdat er meestal meerdere partijen zijn betrokken zowel intern (medische techniek, zorgafdeling, IT) als extern (verschillende leveranciers). Denk hierbij aan:

- eigenaarschap apparatuur, software;
- oplostijden storingen;
- storingen buiten kantoortijden.

Tot slot is het een vereiste om rondom de volgende zaken een risicoanalyse uit te voeren en de benodigde maatregelen te nemen:

- usb-poorten en bijbehorende risico's;
- beschikbaarheid van wifi en het vaste netwerk;
- beheer van apparatuur en netwerk in verband met het oplossen van storingen;
- cybersecurity (zie ook 4.11 *Wat moet ik doen rondom cybersecurity?)*.

De IEC 80001 (geen verplichte norm in Nederland) kan als leidraad worden gebruikt om risicomanagement toe te passen op het netwerk. Zie ook hoofdstuk 4.13 *Wat is de geldende wet- en regelgeving bij medische informatietechnologie?*

IS EEN GESCHEIDEN MEDISCH NETWERK VOOR MEDISCHE APPARATUUR VEILIGER DAN HET ZIEKENHUIS-IT-NETWERK?

Deze vraag heeft helaas geen eenduidig antwoord. Beide opties hebben voor- en nadelen, maar ook risico's, die we hieronder uiteenzetten.
Het ziekenhuis-IT-netwerk gebruiken voor medische toepassingen, zoals patiëntmonitoring (telemetrie) of het hartbewakingsnetwerk, heeft de volgende voordelen:

- de investerings- en exploitatiekosten zijn lager;
- er zijn lagere beheerslasten;
- de interne organisatie geeft mogelijkheid tot kortere responstijden;
- redundantie is over het algemeen beter geregeld;
- de kennis en expertise van de IT-afdeling wordt gebruikt.

Maar zoals gezegd heeft het gebruik van het ziekenhuis-IT-netwerk ook nadelen:

- storingen kunnen ziekenhuisbreed zijn door samenhang van de systemen;
- er is gedeelde verantwoordelijkheid tussen

afdelingen IT en Medische Techniek.
- De capaciteit van het netwerk wordt gedeeld door verschillende toepassingen, waardoor Quality of Service (QoS) op infrastructuur niveau goed ingeregeld moet zijn.

Het gebruik van een gescheiden netwerk voor medische toepassingen heeft als voordeel dat het beheer van medische apparatuur en netwerk bij één partij in het ziekenhuis kan worden belegd. Deze keus brengt echter ook hogere investeringskosten met zich mee.
Het gebruik van het IT-netwerk voor medische toepassingen heeft steeds meer de voorkeur in verband met kosten en functionaliteit (denk aan het uitwisselen van informatie van andere systemen). Welk van beide opties veiliger is, hangt af van vele factoren, ook van het kennis- en expertiseniveau van de medewerkers die het netwerk beheren. Ieder ziekenhuis moet bij elke afweging dus de eigen situatie kritisch bekijken.

HOE ZIT HET MET MEDISCHE APPARATUUR EN WIFI?

Het gebruik van wifi voor de koppeling van medische apparatuur aan een informatiesysteem biedt nieuwe mogelijkheden maar brengt ook risico's met zich mee voor de patiëntveiligheid, effectiviteit en informatiebeveiliging. De praktijkrichtlijn NPR-IEC/TR 80001-2-3: 2012 levert handvatten voor de toepassing van risicomanagement in dergelijke situaties.
Mogelijke oorzaken voor het ontstaan van gevaarlijke situaties zijn bijvoorbeeld RF-interferentie, netwerkuitval of een onjuiste netwerkconfiguratie.
RF-interferentie wordt veroorzaakt door andere draadloze toepassingen of storingsbronnen en is dynamisch van aard. Als door RF-interferentie bijvoorbeeld de koppeling tussen het bewakingssysteem en de smartphone uitvalt, wordt op dat moment een eventuele alarmmelding niet doorgegeven naar de verpleegkundige, met alle risico's van dien. Een beheersmaatregel om een dergelijk risico te beperken is het signaleren van het uitvallen van de verbinding en het direct daarover informeren van de verpleegkundige. Het is dan ook van groot belang om een gedegen multidisciplinaire risicoanalyse op te stellen en van daaruit de nodige beheersmaatregelen te nemen. Zie hiervoor ook hoofdstuk 4.3 *Wanneer moet ik een prospectieve risico-inventarisatie (PRI) uitvoeren?*

Het ontwerpen en aanleggen van een wifi-netwerk vereist naast de nodige IT-kennis ook specifieke kennis van het gedrag van RF-signalen, kennis van andere in gebruik zijnde draadloze toepassingen en de aard van mogelijke storingsbronnen.
Kritische aspecten van een wifi-netwerk zijn onder andere:
- het vereiste dekkingsgebied, dit bepaalt met name het aantal, de ruimtelijke verdeling en de plaatsing van de access points;
- de sterkte van het RF-signaal en de benodigde bandbreedte;
- signalering van uitval van het netwerk;
- de mogelijkheid om QoS (Quality of Service) te gebruiken waarmee hogere prioriteit kan worden toegekend aan de afhandeling van netwerkverkeer van een medische toepassing. Hierbij moet worden opgemerkt dat QoS op het draadloze netwerk niet altijd het gewenste effect geeft, omdat elk draadloos device dat aan het netwerk wordt verbonden zelf een QoS-waarde meegeeft. Zo kunnen bijvoorbeeld telefoons van patiënten en personeel prioriteit vragen en deze ook krijgen;
- fysieke toegankelijkheid van access points; zijn de access points niet zodanig weggewerkt dat het resetten ervan onmogelijk is geworden?

4.8 | HOE RICHT IK WIJZIGINGSBEHEER IN?

De leverancier van medische informatietechnologie kan periodiek nieuwe versies van zijn software uitbrengen. Dit kunnen versies met vernieuwde functionaliteit zijn (upgrade), maar ook met oplossingen voor risicovolle of zelfs gevaarlijke problemen (update). Een leverancier kan in dat geval de gebruiker verplichten de nieuwe versie van de software in gebruik te nemen. Als een nieuwe versie alleen een nieuwe functionaliteit toevoegt die niet van belang is voor de gebruiker, dan kan de gebruiker ervoor kiezen om de update niet door te voeren. Dit moet uiteraard wel gebeuren in overleg met de eigenaar/verantwoordelijke afdelingen, bijvoorbeeld IT, Medische Techniek of Klinische Fysica. Ook moeten hierbij wel de risico's worden afgewogen en moet de leverancier de huidig gebruikte versie nog wel ondersteunen.
Het is daarom van belang om vooraf goede afspraken vast te leggen over het wel of niet doorvoeren van nieuwe versies en de bijbehorende consequenties voor de service en aansprakelijkheid.

WAT VERWACHTEN WE VAN DE LEVERANCIER?

De leverancier heeft zelf verplichtingen bij het ontwikkelen en updaten van zijn software, zoals het uitvoeren van een risicoanalyse, het vastleggen van wijzigingsverzoeken en het informeren over problemen. Het kan echter raadzaam zijn om als gebruiker de leverancier hierover te bevragen om een beeld te krijgen van diens betrouwbaarheid. Maak afspraken dat zonder formele toestemming binnen de eigen organisatie, de leverancier geen softwarewijzigingen mag doorvoeren (bijvoorbeeld gedurende het onderhoud) en leg dit in de inkoopvoorwaarden vast. Bij wijzigingen is het belangrijk om de leverancier te vragen naar mogelijke veranderingen in toepassingsgebied, de intended use. Vraag onder andere naar release notes, beslissing over wijziging, testen en vrijgave, en noodzaak voor trainingen.

EEN NIEUWE VERSIE, WAT DOEN WE NU?

In het geval van het doorvoeren van een update of upgrade van de software moet de fase van ingebruikname opnieuw worden doorlopen. De PRI, die tijdens de aanvankelijke ingebruikname is uitgevoerd, moet worden getoetst met daarbij ook eventueel nieuwe informatie van de leverancier over de risico's. Het kan bijvoorbeeld zijn dat de risicoklasse is gewijzigd, waardoor (ook vanuit de leverancier) een veel uitgebreidere risicoanalyse nodig is.
De aangepaste versie moet in de verschillende beschikbare omgevingen (Ontwikkel, Test, Acceptatie en Productie; OTAP) worden geïmplementeerd en getest. Deze testen kunnen zowel technisch als functioneel van aard zijn. Functioneel gaat het dan om de werking en het gebruik van de software zelf. Technisch moet je denken aan het testen van koppelingen en de integratie met andere systemen, performancetesten en veiligheidstesten. Er moeten daarnaast (nood)procedures ingericht zijn voor het geval van een calamiteit, zowel technisch als functioneel. Voor technische procedures zijn dit bijvoorbeeld back-upsystemen of het redundant uitvoeren van een systeem. Een functionele procedure is meer gericht op de toepassing binnen het zorgproces, bijvoorbeeld op welke pc staat het back-upsysteem en hoe haal ik daar de relevante gegevens vandaan bij een calamiteit?

ITIL, ASL OF...?

Bij het inrichten van een OTAP-omgeving hoort ook een proces om gedurende de levensduur wijzigingen van de medische informatietechnologie goed te borgen. Om dit proces binnen een organisatie goed in te richten geven bijvoorbeeld de procesraamwerken ITIL (Information Technology Infrastructure Library)

en ASL (Application Services Library) een aantal handvatten. ITIL is vooral IT-technisch beheer en ASL is meer voor applicatiebeheer. Beide methodes hebben hun eigen voor- en nadelen, wij adviseren om zoveel mogelijk bij de al in de organisatie aanwezige IT-processen aan te sluiten. Voor ITIL en ASL bestaat diverse literatuur en er zijn specifieke trainingen beschikbaar. Kies vooral een niveau dat binnen de organisatie past. Zie het als een raamwerk en niet als een strikte of letterlijke manier om je processen in te richten.

Binnen het beheerproces worden rollen en verantwoordelijkheden vastgelegd. Dit kan voor de specifieke taken of activiteiten in deze processen bijvoorbeeld gedaan worden met behulp van de RACI-methode (in het Nederlands VERI). Meestal wordt deze uitwerking in tabelvorm vastgelegd, zie als voorbeeld tabel 4.8.1.

WIJZIGINGSBEHEER - RACI

R - Responsible (Verantwoordelijk)
A - Accountale (Eindverantwoordelijk)
C - Consulted (Raadplegen)
I - Informed (Informeren)

ACTIE	Projectleider	Projectteam	Programmamanager	Projectondersteuner	Wijzigingsbeheerder	Change Approval Board
1. Registreer de wijziging in logboek	A	I		I	R	
2. Beoordeel de wijzigingsaanvraag	R/A		I	I	C	
3. Informeer de aanvrager over de uitkomst van de beoordeling	R/A	I		C	I	
4. Stuur de wijziging naar Change Approval Board (CAB)	I	I	C	C	R/A	
5. Controleer de wijziging en keur deze goed of af	I		I	C	C	R/A
6. Informeer stakeholders over uitkomst van CAB besluit	C	I		A	R	
7. Herzie projectplannen, risco's indien nodig	R/A	C		A		
8. Update wijzigingslogboek	A	I	I	I	R	I
9. Update programmaplan	C		R/A	I		
10. Implementeer de wijziging	A	R	C	C	I	I

Tabel 4.8.1. Rollen en verantwoordelijkheden in het wijzigingsbeheerproces

HOE GAAT DIT BIJ EEN SAMENGESTELD SYSTEEM, BIJVOORBEELD EEN MEDISCH ALARMERINGSSYSTEEM (MA)?

Elke wijziging van een onderdeel van het systeem kan direct invloed hebben op de andere onderdelen en de samenwerking van de onderdelen. In het geval van een MA is een wijziging van software van een medisch apparaat bijvoorbeeld van invloed op de communicatie of het uitsturen van alarmen. Als een wijziging ervoor zorgt dat bijvoorbeeld meer of minder alarmen uitgestuurd worden door het apparaat, moeten de verschillende partijen deze wijziging beoordelen op wenselijkheid. Vervolgens moeten de risico's in kaart gebracht worden. Als het licht dan nog steeds op groen staat, kan de wijziging doorgevoerd worden voor één apparaat en vervolgens met de testomgeving van het MA getest worden. Zodra dit akkoord is, kan de wijziging definitief worden gemaakt en bij eventueel andere apparaten doorgevoerd worden. Scholing van het personeel kan noodzakelijk zijn. Ook is het belangrijk dat al deze wijzigingen gedocumenteerd worden in een systeemdossier bij de betreffende component. Vaak moeten veel verschillende partijen de wijziging beoordelen voordat die doorgevoerd kan worden, zoals de afdelingen Medische Techniek, Klinische Fysica, Klinische Informatica, Infra en IT (vaak diverse organen binnen de IT-afdeling). Maar ook leverancier A, leverancier B, gebruikers/eigenaar afdeling I, gebruikers/eigenaar afdeling II, et cetera.
Naast softwarewijzigingen is het bij samengestelde systemen belangrijk om ook infrastructurele wijzigingen te beoordelen. Deze wijzigingen zijn vaak onvoldoende in het vizier. Denk bijvoorbeeld aan het veranderen van het type access points voor wifi, andere servers of switches. Bij aanschaf en installatie is het van belang dat alle partijen aangeven wat de vereisten zijn voor de infrastructuur. Dit moet vastgelegd worden in het systeemdossier (CMDB). Bij wijzigingen aan de infrastructuur moet duidelijk worden of en welke consequenties dit heeft voor het systeem. Een toetsing bij de leveranciers van deze aanpassingen is een must.
Alle componenten van het systeem hebben periodiek onderhoud nodig. Deze periodes liggen helaas niet allemaal gelijk. Het is belangrijk om dit onderhoud zoveel mogelijk te coördineren zodat het zorgproces zo min mogelijk hinder ondervindt. Het is volstrekt onaanvaardbaar als een kritisch systeem zoals het MA in week 1 'plat ligt' door onderhoud aan component A, in week 2 door onderhoud aan component B en in week 3 door wijziging van softwarecomponent C. Een coördinerende rol om deze werkzaamheden op elkaar af te stemmen ligt doorgaans bij één partij in de zorginstelling.
Na elke wijziging die doorgevoerd wordt aan het systeem moet een standaard testplan uitgevoerd worden. Een voorbeeld van een testplan voor het MA staat in tabel 4.8.2.

HOE MOET IK WIJZIGINGSBEHEER INRICHTEN ALS IK ZELF SOFTWARE ONTWIKKEL?

In hoofdstuk 4.1 *Waar moet ik aan denken als ik zelf software wil ontwikkelen?* staat in welke mate 'in huis' ontwikkelde software moet voldoen aan de MDR vanaf 2020. Hierin is de tweedeling beschreven, ofwel volledig voldoen aan de MDR, ofwel gedeeltelijk. Hoewel er op dit moment onder de MDD geen duidelijkheid is aan welke voorwaarden moet worden voldaan, is het voor het wijzigingsbeheer raadzaam al rekening te houden met de toekomstige verplichtingen van de MDR.
Voor zelfontwikkelde software die volgens het bovengenoemde artikel gedeeltelijk onder de MDR valt, staat het een zorginstelling vrij om dit volledig binnen de eigen wijzigings-beheeromgeving op te nemen. Het is nu wel de verplichting van de zorginstelling om

een periodieke risicoanalyse uit te voeren, wijzigingsverzoeken en beslissingen hierover vast te leggen, release notes te documenteren, gebruikers te informeren over problemen met de software en test- en vrijgaveprocedures vast te leggen. Bij wijzigingen is het belangrijk om na te gaan of de intended use verandert en of de gebruikers aanvullende training nodig hebben. Voor updates geldt de hier eerder genoemde informatie onder het kopje ‘Een nieuwe versie, wat doen we nu?’
Als de software toch op alle punten aan de MDR moet voldoen, bijvoorbeeld omdat er al een vergelijkbaar product op de markt is, moeten er aanvullende maatregelen genomen worden. In het softwareontwikkelplan wordt dan het wijzigingsbeheerproces beschreven. Voor verdere details en uitwerking van dit plan, zie het eerdergenoemde artikel en IEC 62304.

Basisplan voor alle afdelingen nog apart nodig om te testen op alarminstellingen.

- Benodigdheden: kamer met bewakingsmonitor en twee handhelds die je kunt toewijzen aan de kamer als eerste verantwoordelijke en als buddy.
- Pak het alarmoverzicht van de afdeling waarop staat welke alarmen doorgestuurd worden en hoe er doorgestuurd wordt (naar buddy of naar iedereen).
- Voer onderstaande testen uit om te controleren of de alarmering weer functioneel is.
- Indien bewakingen centraalpost niet uitgevallen zijn, hoeft de test maar op één handheld met één bewakings-monitor uitgevoerd te worden.

		Let op, deze kolom verschilt per afdeling	Deze kolom invullen op de gele vlakken
	Datum van de test_____ **Uitvoerder van de test**_____		
	Wat je moet testen: beschrijving	**Setting moet zijn**	**Setting bij test is**
1.	Komt een urgent, rood alarm (Philips) of crisis alarm (GE) van bewakingsmonitor op handheld?	Ja	
2.	Is het duidelijk om welk alarm het gaat (tekstbericht is duidelijk)?	Bijvoorbeeld Asystole	
3.	Komen de vitale parameters van de patiënt mee in het tekstbericht?	Bijvoorbeeld HR 60	
4.	Komt het juiste kamernummer mee in het tekstbericht?	Ja	
5.	Komt een grensoverschrijdend, geel of bedreigend alarm van bewakingsmonitor op handheld?	Nee	
6.	Welke keuzeopties zijn mogelijk op de handheld bij een bewakingsmonitor-alarm (denk aan confirm, accept, busy)?	Accept en busy (op rood alarm)	
7.	Komt een alarm van VOS-MOS-MA op handheld?	Ja	
8.	Komt het juiste kamernummer mee in het tekstbericht?	Ja	
9.	Welke keuzeopties zijn mogelijk op de handheld bij een alarm van VOS-MOS-MA (denk aan confirm, accept, busy)?	Accept en busy (op rood alarm)	
10.	Werkt het toewijzen van de toestellen voor zowel medische alarmering als VOS-MOS?	Ja	
	De volgende testen worden alleen uitgevoerd voor een bewakingsmonitor-alarm, pak hiervoor een asystolie alarm (of welk alarm kan het best hiervoor gekozen worden: gebruiker moet dit eenvoudig zelf kunnen testen):		
11.	Is escalatievia de handheld mogelijkdoor op de knop busy te drukken? (Alleen voor MMGAscom)	Ja	
12.	Als op busy gedrukt wordt, na hoeveel seconden gaat het alarm dan naar de tweede handheld?	< 10 seconden	
13.	Als dan op tweede handheld ook op busy gedrukt wordt, na hoeveel seconden gaat het alarm dan naar de derde escalatie (alle seinen)? Dit is alleen van toepassing bij GE/ Ascom.	< 10 seconden	
14.	Als het alarm genegeerd wordt, na hoeveel seconden gaat het alarm dan naar de tweede handheld?	< 50 seconden	
15.	Als het alarm geaccepteerd wordt maar niet wordt weggedrukt op de bewakingsmonitor, na hoeveel seconden gaat het alarm dan naar de eerste en tweede handheld?	< 60 seconden	
16.	Wat gebeurt er als de eerste handheld niet toegewezen is?	Direct op buddy	
17.	Wat gebeurt er als de eerste handheld uitstaat?	Direct op buddy	
	De volgende testen worden alleen uitgevoerd voor een VOS-alarm (patiëntbel)		
18.	Is escalatie via de handheld mogelijk door op de knop busy te drukken? Alleen bij GE/Ascom.	Ja	
19.	Als op busy gedrukt wordt, na hoeveel seconden gaat het alarm dan naar de tweede handheld?	< 10 seconden	
20.	Als dan op tweede handheld ook op busy gedrukt wordt, na hoeveel seconden gaat het alarm dan naar de derde escalatie? Alleenbij GE/Ascom, alle seinen	< 10 seconden	
21.	Als het alarm genegeerd wordt, na hoeveel seconden gaat het alarm dan naar de t weede handheld?	< 10 seconden	
	Als er apparatuur gekoppeld is aan monitor		
22.	Komen de rode alarmen van de Fabian HFO beademingsmachine (alleen NICU) door op de handheld?	Ja	
23.	Komen de alarmen van de infusie door op de handheld?	Ja	
24.	Is er verschil te zien tussen rode en gele alarmen?	Ja	

Tabel 4.8.2. Testplan alarmen na onderhoud

4.9 | WELKE BEHEERAFSPRAKEN MOET IK MAKEN MET WELKE PARTIJEN?

Medische informatietechnologie zoals besproken in deze Praktijkgids bestaat veelal uit medische- en niet-medische apparatuur en IT-infrastructuur. Bij het beheer van een dergelijke technologie zijn dan ook altijd meerdere partijen betrokken. Denk hierbij aan gebruikers, aan de afdelingen IT, Medische Techniek, Klinische Fysica, Klinische Informatica en aan externe leverancier(s).
Om de medische informatietechnologie te beheren moeten er allerlei zaken worden geregeld en afspraken worden gemaakt, zoals gebruikersondersteuning, oplossen van storingen, periodiek onderhoud en het doorvoeren van wijzigingen in het systeem. Binnen veel zorginstellingen bestaan er tussen de zorgafdelingen en ondersteunende afdelingen als IT en Medische Techniek al afspraken of overeenkomsten waarin de standaard dienstverlening is beschreven. Om beheerafspraken te maken voor een specifieke medische informatietechnologie is het handig en praktisch om aansluitend op deze bestaande afspraken of overeenkomsten aanvullende operationele afspraken en procedures op te stellen en op te nemen in een DAP (Dossier Afspraken en Procedures). Als er tevens sprake is van een onderhoudsovereenkomst met een externe leverancier, worden ook de operationele afspraken over de uitvoering van deze overeenkomst opgenomen in het DAP. Met alle informatie in het DAP weten alle betrokken partijen in detail wat er van hen wordt verwacht en hoe er moet worden samengewerkt. In bijlage XI staat een goed voorbeeld van zo'n DAP. [24]
Het is van belang al in de verwervingsfase over het toekomstige beheer na te denken en van hieruit eisen op te nemen in het Pakket van Eisen voor de verwerving. Denk bijvoorbeeld aan noodzakelijke opleidingen en trainingen, mogelijke onderhoudscontracten, software-updates en technische documentatie. Idealiter is het beheer geregeld en operationeel zodra een medische informatietechnologie daadwerkelijk in gebruik wordt genomen. Op dat moment moet het voor de gebruikers duidelijk zijn bij wie ze storingen kunnen melden en welke dienstverlening ze mogen verwachten van de ondersteunende afdelingen. Ook moeten de ondersteunende afdelingen als Medische Techniek en IT (functioneel beheer, technisch beheer, technisch applicatiebeheer) maar evengoed de gebruikers hun rol kennen en kunnen uitvoeren en moeten eventuele onderhoudscontracten met externe leveranciers in werking zijn.
Om afspraken te maken over dienstverlening (intern of extern) en onderhoud (extern) kan men gebruikmaken van een DVO (Dienst Verlening Overeenkomst) ook wel SLA (Service Level Agreement) genoemd of een SSO (Standaard Service Overeenkomst). Tussen de termen DVO en SLA bestaat in de praktijk geen verschil, we hanteren hier verder de term SLA.

Tussen een SLA en een SSO zit wel een verschil. Met beide kun je onderhoud regelen, het verschil zit in de invalshoek: de SLA focust op de services en servicelevels en de SSO focust op het onderhoud waar uiteraard ook eisen aan gesteld worden. Als het accent vooral ligt op onderhoud van een specifiek apparaat, adviseren we de SSO te gebruiken omdat die voor dit doel al in verregaande mate is uitgewerkt.

[24] *Zie bijlage XI Dossiers, Afspraken en Procedures (DAP) op www.mtintegraal.nl*

WAT STAAT ER IN EEN SLA?

Een SLA is een overeenkomst tussen een opdrachtgever en een opdrachtnemer waarin afspraken worden opgenomen over de levering van producten en diensten en waarin de wederzijdse verantwoordelijkheden worden vastgelegd. In een SLA worden aan te onderscheiden services bepaalde service levels, ook wel prestatieniveaus, gekoppeld. Door de geleverde services te monitoren wordt bepaald in hoeverre een leverancier zijn afspraken nakomt en kan deze waar nodig worden bijgestuurd. In een SLA kunnen ook afspraken worden opgenomen over kosten en eventuele sancties wanneer een leverancier de gemaakte afspraken niet of onvoldoende nakomt.

Eenvoudige voorbeelden van mogelijke services en service levels in een SLA zijn:

- beschikbaarheid van een systeem 99,5 % over de jaaruren (24x7x365);
- bereikbaarheid van de helpdesk 7x24 uren;
- oplostijd van urgente storingen van maximaal 3 klokuren.

In een SLA kan daarnaast ook een verwijzing worden opgenomen naar een specifieke onderhoudsovereenkomst, naar inkoopvoorwaarden, naar leveringsvoorwaarden of naar Producten en Diensten Catalogus (PDC). In een PDC staat de standaard dienstverlening van een serviceverlener beschreven. In een SLA voor een medische informatietechnologie wordt ook een verwijzing opgenomen naar een specifieke DAP. In het DAP worden de zaken opgenomen waarmee een leverancier nadere invulling geeft aan de in de SLA gemaakte afspraken. Ook afspraken over communicatie en samenwerking tussen alle betrokken partijen worden opgenomen in het DAP.
SLA's worden wel afgesloten tussen zowel interne partijen als tussen een interne en een externe partij. Een voorbeeld van een interne SLA is een overeenkomst tussen een zorgafdeling en de afdeling Medische Techniek over het beheer en onderhoud van de medische apparatuur. Een voorbeeld van een externe SLA is een overeenkomst tussen een zorginstelling en een externe leverancier over het beheer en onderhoud van een PACS.
Voor een goed servicemanagement is het van belang om de gemaakte afspraken regelmatig te evalueren aan de hand van rapportages over de geleverde prestaties. In hoeverre komt een leverancier de gemaakte afspraken na? Zijn er knelpunten gesignaleerd in de dienstverlening? Het is ook mogelijk dat risico's in de loop van de tijd wijzigen of dat de praktijk uitwijst dat bepaalde risico's niet of onvoldoende waren onderkend. Ook kan het nodig blijken om procedures of werkafspraken aan te passen.

HOE STEL IK EEN SLA OP?

Het opstellen van een SLA vereist altijd maatwerk. Als je een SLA wilt opstellen voor medische informatietechnologie is het van belang dat eerst de risico's van het systeem in kaart zijn gebracht en er maatregelen zijn vastgesteld om deze risico's te beheersen. Ook moet duidelijk zijn welke eisen de gebruiker stelt, welke rol de afdelingen IT en Medische Techniek in het beheer kunnen spelen en of er ook externe ondersteuning nodig is. Deze informatie vormt de basis voor een op te stellen SLA. Op de website van ZBC kennisbank [25] staat een checklist met de belangrijkste onderdelen en aandachtspunten om een SLA op te stellen. Op meerdere websites zijn daarnaast formats te vinden waarmee een SLA en DAP kan worden gemaakt. [26]

HOE STEL IK EEN ONDERHOUDS-OVEREENKOMST OP?

Om afspraken te maken met een leverancier over onderhoud aan apparatuur, software en systemen kan je in veel gevallen gebruikmaken van de Standaard Service Overeenkomst (SSO) van de WIBAZ/FHI/NEVI. Deze SSO is modulair opgezet en kent onder andere modules voor periodiek onderhoud, uptime garantie, software-updates en -upgrades en een module voor remote service. De SSO en het bijbehorende invuldocument kunnen worden gedownload van de site. [27]

[25] *https://zbc.nu/ict/kwaliteit-ict-beheer-itil-en-sla/checklist-service-level-agreement-sla/*

[26] *Zie bijlage XII Checklist Service Level Agreement (SLA) op www.mtintegraal.nl*

[27] *https://www.wibaz.nl/mdocs-posts standaard-service-overeenkomst-2016/*

4.10 | HOE VALIDEER IK SOFTWARE EN WAT HEB IK DAN AAN EEN OTAP?

Voor de ingebruikname van een medische informatietechnologie is het noodzakelijk om het functioneren van de software te valideren. Het doel van deze validatie is controleren of de technologie werkt volgens de opgegeven specificaties in de ziekenhuisomgeving.
De FDA hanteert de volgende definitie voor softwarevalidatie: 'confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled.' [28]
Het is dus de bedoeling om te controleren of de medische informatietechnologie voldoet aan de door de gebruiker opgestelde functionele specificaties.

WAT STAAT ER IN DE LITERATUUR OVER SOFTWAREVALIDATIE?

In Engeland is er een nationale groep, de Nuclear Medicine Software Quality Group (NMSQG) die als doel heeft om landelijk softwarepakketten voor nucleaire geneeskunde met elkaar te vergelijken, onder andere door testbeelden te verstrekken en de resultaten van de verschillende pakketten met elkaar te vergelijken. In Nederland is er door de NCS (Nederlandse Commissie voor Stralingsdosimetrie) een rapport opgesteld waarin de validatie van treatment planning systemen wordt beschreven.[29] Voor het opstellen hiervan is gebruikgemaakt van al aanwezige AAPM-rapporten (American Association of Physics in Medicine), waarbij in de NCS-rapporten praktische invulling wordt gegeven aan de testen die benoemd worden in het AAPM-rapport. Dit NCS-rapport kan ook gebruikt worden als inspiratie om een validatieprotocol op te stellen voor andere softwarepakketten.

HOE DOE IK DE SOFTWAREVALIDATIE?

Door de leverancier zijn al diverse tests gedaan om de medische software (standalone of onderdeel van een medisch systeem) te valideren. De validatie door het ziekenhuis start bij het opvragen van de resultaten van deze tests bij de leverancier. Als de omgeving waarin de medische software gebruikt wordt niet van invloed is op de resultaten van deze tests, hoeven deze niet nogmaals uitgevoerd te worden.
Voor het goed uitvoeren van de validatie is het noodzakelijk om een testomgeving te hebben die gelijk is aan de werkelijke productie-omgeving. Soms is het mogelijk om nieuwe medische software veilig in de productie-omgeving te testen, bijvoorbeeld doordat toegang tot de software afgeschermd is met een wachtwoord dat alleen toegankelijk is voor geautoriseerde personen en de software geen invloed heeft op de werking van andere systemen. Indien beide niet mogelijk zijn, moet er gekeken worden naar alternatieven. De mogelijkheden hierbij zijn afhankelijk van het type medisch software en de toepassing.
Voorafgaand aan de validatie moet door de projectgroep een validatieprotocol opgesteld worden. Dit is gebaseerd op het Pakket van Eisen (PvE), dat in de verwervingsfase is opgesteld, en de risicoanalyse.
Om een goed validatieprotocol op te kunnen stellen, is het noodzakelijk dat bekend is hoe er met de software gewerkt gaat worden, zodat ook met de juiste configuratie getest kan worden.
Tijdens de validatie kunnen diverse hulpmiddelen worden gebruikt. Denk hierbij aan fantomen, simulaties van bepaalde situaties, vrijwilligers (alleen als dit zonder risico is voor de vrijwilliger), testbeelden, referentie-datasets en testapparatuur.

Een voorbeeld van een test die bij de softwarevalidatie uitgevoerd kan worden is het testen of volumes goed berekend worden door de software. Dit kan bijvoorbeeld gedaan worden door een fantoom met bekende volumes te scannen en de software de volumes te laten berekenen.

WAT IS DE TOEGEVOEGDE WAARDE VAN EEN OTAP VOOR DE VALIDATIE?

Om het product te kunnen testen en te valideren wordt vaak een OTAP-omgeving ingericht. Dit acroniem staat voor:

- Ontwikkelomgeving (meestal alleen bij de fabrikant)
- Testomgeving (onderdeel van de initiële installatie)
- Acceptatieomgeving (een recente kopie van de Productieomgeving inclusief de koppelingen)
- Productieomgeving (de uiteindelijke productieomgeving)

Deze omgevingen zijn virtueel en/of fysiek van elkaar gescheiden.
Voor validatie/verificatie van medische software is het noodzakelijk om naast de productie (klinisch gebruik) ook een acceptatieomgeving beschikbaar te hebben. Het is belangrijk dat de acceptatieomgeving een representatieve kopie van de productieomgeving is. Denk dus ook aan de gekoppelde randapparatuur en/of interne en externe datakoppelingen.

Zonder OTAP-omgeving is het vaak lastig om software te valideren. De softwarevalidatie kan dan alleen in de productieomgeving (dus de klinische omgeving) plaatsvinden. Dit kan alleen veilig plaatsvinden als het mogelijk is om de nieuwe en oude software tijdelijk naast elkaar te laten lopen en klinische beslissingen te baseren op de oude software, zolang de nieuwe software niet gevalideerd is. Validatie van de software is in de productieomgeving lastiger dan in de testomgeving, doordat de testomstandigheden minder gecontroleerd zijn.

WAT ZIJN BELANGRIJKE AANDACHTSPUNTEN BIJ HET OPSTELLEN VAN EEN VALIDATIEPROTOCOL?

Bij het opstellen van het validatieprotocol zijn de volgende zaken van belang:

- Betrek alle relevante disciplines bij het opstellen van het protocol. Denk hierbij aan: de afdelingen Medische Techniek, Klinische Fysica, IT (netwerkbeheer en databasebeheer), Klinische Informatica, en de gebruiker.
- Test zowel standaardsituaties als extreme situaties en noodsituaties.
- Bedenk vooraf wanneer de resultaten van de validatietest acceptabel zijn en wanneer niet.
- Test alle koppelingen en interfaces.
- Controleer welke loggingmogelijkheden de software heeft.
- Controleer of alle foutmeldingen en/of alarmen werken en duidelijk zijn.
- Performance-testen.
- Beveiliging.
- Instellingen (landeninstellingen, eenheden, formats (bijvoorbeeld datumformats, decimaaltekens, tijdinstellingen).
- Bevoegdheden/toegang/licenties.

Het is onmogelijk om een medische informatietechnologie volledig te testen. Daarom is het noodzakelijk om tijdens het opstellen van het validatieprotocol goed na te denken welke zaken zeker getest moeten worden.

[28] *Zie info bij geraadpleegde bronnen.*

[29] *https://doi.org/10.25030/ncs-015*

4.11 | WAT MOET IK DOEN RONDOM CYBERSECURITY?

Cybersecurity is een hot topic op dit moment, dat blijkt alleen al uit de jaarlijkse top-10 Health Technology Hazards van het ECRI Institute waarin de laatste jaren de risico's omtrent IT een steeds prominentere rol spelen. Diverse regelgevingen verplichten zorginstellingen om deze risico's goed af te dekken. Er komt geregeld een bericht in het nieuws dat patiëntgegevens gelekt zijn of afdelingen van ziekenhuizen tijdelijk gesloten zijn wegens computerstoringen.
Als een dergelijk incident voorvalt, kan dit grote gevolgen hebben voor patiënten: de privacy van de patiënt kan in het geding zijn, maar ook de patiëntveiligheid kan in gevaar komen. Dit kan voor het imago van de zorginstelling een flinke klap betekenen.
Cybersecurity draait om een drietal componenten. Data moeten beschikbaar, integer en vertrouwelijk zijn. De beschikbaarheid van data is cruciaal voor de patiëntenzorg. Als patiëntgegevens niet beschikbaar zijn, wordt de zorg tijdelijk op de hele afdeling of zelfs de hele zorginstelling stilgelegd. Als patiëntgegevens niet integer zijn, betekent dit dat de data niet juist zijn. Als bijvoorbeeld de CT-scan bij een verkeerde patiënt staat geregistreerd kan dit desastreuze gevolgen hebben. De vertrouwelijkheid van data is belangrijk voor de privacy van de patiënt. Patiëntgegevens mogen niet in verkeerde handen komen. Inmiddels is de medische sector voor hackers erg interessant geworden.

De NEN 7510 (vanuit ISO 27001, ISO 27002 en ISO 27799) bevat veel verschillende aandachtspunten om verantwoorde zorg te leveren met een adequate beveiliging van de patiëntgegevens. In de toetsingscriteria staat een handreiking waarmee een organisatie getoetst wordt en waarmee ook een zelfevaluatie uitgevoerd kan worden. In die handreiking is ook toegevoegd wat specifiek voor medische apparatuur van toepassing is ten opzichte van alle criteria voor de andere medische informatietechnologie. De koppeling van medische apparatuur aan IT-netwerken maakt dergelijke systemen kwetsbaarder voor virussen en ongeautoriseerde toegang wat tot risico's met zich meebrengt. Het is raadzaam om de gehele norm voor de organisatie van een bepaalde medische informatietechnologie door te lopen.

WAT KAN IK ONDERVANGEN BIJ DE SELECTIE VAN MEDISCHE SYSTEMEN?

In de verwervingsfase van medische systemen is het belangrijk dat er op een aantal punten aandacht is voor cybersecurity. Het MDS2-formulier kan hiervoor een hulpmiddel zijn (bijlage XIII).[30] Potentiële leveranciers vullen dit formulier in om informatie te verschaffen over security-aspecten. Deze aspecten kunnen dan goed beoordeeld worden.

Een aantal belangrijke vragen die zijn opgenomen zijn:

- Verstuurt het apparaat patiëntgegevens?
- Heeft het apparaat exportmogelijkheden naar draagbare media (usb, dvd, et cetera)?
- Welke communicatiemechanismen gebruikt het apparaat (bijvoorbeeld LAN, WLAN, VPN, IEEE1073, usb, firewire, bluetooth, wifi of infrared)?
- Welk operating system gebruikt het apparaat?
- Wat zijn de back-upmogelijkheden?
- Wat zijn de boot-mogelijkheden?
- Is het mogelijk om op afstand in te loggen?
- Is het mogelijk om audit trails te genereren? Is er een inlog per gebruiker mogelijk, eventueel door scannen van een personeelspas bij belangrijke handelingen?
- Kan het systeem geüpdatet worden?

[30] *Zie bijlage XIII MDS2-formulier op www.mtintegraal.nl.*

- Beschikt het systeem over een virusscanner of is de installatie hiervan mogelijk?
- Kan het apparaat netwerkverkeer versleutelen?
- Ondersteunt het apparaat encryptie naar media en borgt het de integriteit van deze data?

Het kan daarnaast goed zijn om een aantal punten al in het Pakket van Eisen op te nemen, bijvoorbeeld bij een Europese aanbesteding. Het gaat dan om:

- de IT-infrastructuureisen van de zorginstelling om zo mogelijk aan te sluiten bij de standaard IT-infrastructuur;
- de mogelijkheid tot encryptie van data;
- gebruik van WPA2 als wifi wordt gebruikt;
- een up-to-date virusscanner op het systeem;
- het tijdig doorvoeren van up-to-date patches van OS en software;
- de redundantie van servers en
- de eis dat de leverancier geaccrediteerd is voor NEN 7510 (ISO 27001 en ISO 27002/27799).

HOE KAN IK MEDISCHE INFORMATIE-TECHNOLOGIE BEVEILIGEN?

Medische apparatuur of medische software wordt vaak in een bepaalde configuratie geleverd die gebruikt is tijdens de CE-certificering van het medisch hulpmiddel. Dit betekent vaak dat elke patch van bijvoorbeeld het Operating System (OS) eerst door een validatieproces gehaald moet worden door de leverancier. Regelmatig is het zelfs zo dat de leverancier geen patching doet op het geleverde systeem en ook geen virusscanning toelaat op het medische apparaat of de pc/server met medische software. De apparatuur en applicatie zijn dan erg kwetsbaar.

Om medische informatietechnologie toch te beveiligen bij afwezigheid van virusscanning of achterstalligheid in patching, kan de hardware in een apart (medisch) VLAN geplaatst worden, achter een firewall met IPS-functionaliteit (Intrusion Protection System). De firewall controleert vervolgens alle verkeer van en naar het VLAN waardoor het VLAN voor de buitenwereld is afgeschermd.
Nadeel van het plaatsen van kwetsbare hardware in een VLAN is dat besmetting die eenmaal in het VLAN zit zich makkelijk kan verspreiden onder de kwetsbare apparatuur. Dit betekent dat bijvoorbeeld het gebruik van usb-sticks sterk gereguleerd moet worden. In principe is het het beste om het gebruik van usb-sticks te verbieden op deze kwetsbare apparatuur en hiervoor de usb-poorten af te sluiten. Het is echter soms nodig om usb-sticks of aansluiting van service laptops via usb-poorten toe te staan voor servicedoeleinden. Deze usb-sticks moeten dan vooraf gecontroleerd worden op virussen op een pc met adequate virusbeveiliging. De service laptops moeten ook voorzien zijn van deze adequate virusbeveiliging.

Als updates doorgevoerd kunnen en moeten worden, regel dit dan via een wijzigings-procedure. Meer over de methodes om dit te organiseren staat in hoofdstuk 4.8 *Hoe richt ik wijzigingsbeheer in?* In ieder geval worden, als dat mogelijk is, wijzigingen eerst in de OTA (Ontwikkel, Test, Acceptatie)-omgeving getest voordat ze in de productie worden doorgevoerd. Zie voor de inrichting van OTAP (Ontwikkel, Test, Acceptatie, Productie) hoofdstuk 4.6 *Wat is een OTAP en wat is het nut daarvan?*
De inrichting van remote service (voor wijzigingen en beheer) met de leverancier van medische informatietechnologie is ook erg belangrijk. Maak goede afspraken met de leveranciers wanneer en hoe de leverancier remote service kan verlenen. Om remote service veilig in te richten is een VPN-verbinding (Virtual Private Network) nodig en een token om de leverancier gecontroleerd toegang te verlenen. Log ook alle acties die gedaan zijn via deze VPN.

Beschikbaarheid van dataverkeer wordt een steeds belangrijker aandachtsgebied nu veel systemen met elkaar gekoppeld worden.
Zo is het verkeer van medische apparatuur via het netwerk cruciaal voor de zorg. Om belangrijk dataverkeer voorrang te geven kan het netwerk met Quality of Service (QoS) ingericht worden. Meestal wordt dan met het datapakketje een prioriteitsgetal meegegeven. Het is wel van belang dat apparatuur met deze technologie kan werken. Daarnaast is het geen sluitende garantie dat dataverkeer met hoge prioriteit voorrang krijgt. De leverancier van een product bepaalt het prioriteitsgetal. Zo kan een consumentenproduct ook een hoog prioriteitsgetal krijgen als het bijvoorbeeld afhankelijk is van continu streamen waardoor de prioriteit gelijk wordt aan het cruciale medische dataverkeer.

Om medische applicaties gedurende het testen van de productieomgeving te isoleren/beveiligen wordt vaak gebruikgemaakt van een zogenaamde zandbak of sandbox. Dit is een beveiligde werkomgeving waarbij de te testen applicatie geen verstoring van de productie kan geven en tegelijkertijd afgeschermd is voor malware of virussen. Een zandbak kan ook als leer- en oefenomgeving voor gebruikers worden gebruikt.

HOE GA IK OM MET TOEGANKELIJKHEID VAN MEDISCHE INFORMATIETECHNOLOGIE?

Om te zorgen dat de medische informatietechnologie alleen toegankelijk is voor daartoe bevoegde personen, zijn er enkele beveiligingseisen aan verbonden.
De medische software moet met persoonsgebonden authenticatie en autorisatie te benaderen zijn waarbij de acties op en het inzien van data gelogd moet worden zodat ze tot individuele gebruikers te herleiden zijn.
Het gebruiken van de medische software zit dan achter een wachtwoord dat regelmatig gewijzigd moet worden. Maak een goed onderbouwde afweging voor uitzonderingen hierop. Zo zien we in veel zorginstellingen dat de medische apparatuur te gebruiken is zonder wachtwoord of met een algemeen wachtwoord. Er moet een risicoafweging gemaakt worden voor het niet tijdig en/of handig kunnen gebruiken van een medisch apparaat ten opzichte van het afschermen van de medische software.
Met Enterprise Single Sign-On (ESSO) is de medische software op een makkelijke manier af te schermen. Dit werkt echter meestal (nog) niet bij medische apparatuur.
Om de hardware (servers, pc's, medische apparatuur, IT-infrastructuur) te beschermen moet de hardware zoveel mogelijk in een fysiek afsluitbare ruimte geplaatst worden. Alleen geautoriseerde personen kunnen zo bij de hardware.

Medische software heeft vaak diepere lagen die voor de klinische gebruikers afgeschermd moeten zijn omdat hier technische instellingen of de kern van de applicatie aangepast kunnen worden. Deze diepere lagen moeten beschermd worden met wachtwoorden die geregeld gewijzigd worden. Helaas zien we vaak dat men de fabriekswachtwoorden gebruikt, die voor alle instellingen gelijk zijn. Bekijk met de leverancier of deze wachtwoorden aangepast kunnen worden.
Omdat de bescherming erg afhankelijk is van de acties van gebruikers is scholing met de nadruk op bewustwording een belangrijke stap. Stel als basis hiervoor een beleid op waarin staat dat gebruikers regelmatig hun wachtwoorden moeten wijzigen en waaraan die wachtwoorden moeten voldoen. Neem in dit beleid ook mee dat de gebruikers de werkstations en apparatuur moeten afsluiten of vergrendelen zodra ze de medische software niet meer gebruiken. Geef ook aan dat de gebruiker de fysieke ruimte waarin pc's en medische apparatuur staan, moet afsluiten bij het verlaten van deze ruimte.
Voor medische apparatuur is de bescherming lastig. Het is bijvoorbeeld vaak praktisch niet haalbaar om de software voor klinische gebruikers via wachtwoorden te beschermen of om fabriekswachtwoorden voor afscherming van technische instellingen te wijzigen. Het is van belang om hierover wel in gesprek te gaan met de leveranciers om te kijken of dit op termijn, via een voor de kliniek acceptabele manier, te realiseren is.
Als de wachtwoorden van medische apparatuur (gebruikers, technische instellingen, kernsoftware) gewijzigd kunnen worden, is het belangrijk om hier iemand verantwoordelijk voor te maken die dit periodiek doet. Deze taak kan bijvoorbeeld goed liggen bij de medische instrumentatietechnicus van het medische apparaat.

WAT KAN IK NOG MEER REGELEN?

Om te voorkomen dat data na het afvoeren van hardware in verkeerde handen vallen, moeten deze zo mogelijk van de hardware verwijderd worden door destructie van de harde schijf.
Laat de leverancier een vernietigingsverklaring opstellen als hij de enige is die de patiëntgegevens van de hardware kan verwijderen.

Leveranciers van medische informatietechnologie komen vaak in aanraking met de software en medische gegevens van patiënten. Daarom is het belangrijk afspraken te maken met leveranciers over geheimhouding. Dit kan in de vorm van een verwerkersovereenkomst. Een verwerkersovereenkomst is een overeenkomst waarin afspraken zijn opgenomen over het verwerken van persoonsgegevens door een derde partij. Een dergelijke overeenkomst is verplicht vanuit de Wbp (Wet bescherming persoonsgegevens) en AVG (Algemene verordening gegevensbescherming), die stellen dat een organisatie verplicht is maatregelen te nemen om de privacy van persoonsgegevens te beschermen. Dit betreft niet alleen patiëntgegevens maar ook gegevens van bijvoorbeeld medewerkers. Een organisatie blijft hiervoor verantwoordelijk, ook als zij bepaalde diensten door een derde partij laat uitvoeren.
In een verwerkersovereenkomst worden daarvoor eisen en afspraken opgenomen. Denk hierbij bijvoorbeeld aan informatiebeveiliging, geheimhouding van informatie, melding van incidenten, interne controle en eisen aan certificering.
De NVZ heeft een template voor de verwerkersovereenkomst opgesteld. [31]

Naast een goede implementatie van beveiligingsmaatregelen en de instructie voor de medewerkers, is het erg belangrijk om een kwetsbaarheid te signaleren. Enerzijds kan dit gedaan worden door de signalering via ketenmonitoring per medisch systeem zodat er continue monitoring plaatsvindt op de Beschikbaarheid, Integriteit en Vertrouwelijkheid van de data. Anderzijds is het goed om op de hoogte te blijven van gevonden kwetsbaarheden. Leg een melding van een kwetsbaarheid vast in de verwerkersovereenkomst met de leverancier. Het is daarnaast ook van belang om beveiligingsmeldingen te volgen.
Deze meldingen worden gedaan door bijvoorbeeld het ECRI Institute of door het recent opgerichte Z-CERT. Het Z-CERT ondersteunt zorginstellingen op het gebied van cybersecurity, onder andere door de deelnemers te informeren over kwetsbaarheden bekend bij het Z-CERT.

WAAR KAN IK MEER INFORMATIE VINDEN?

Voor meer informatie over adequate beveiliging van persoonsgegevens verwijzen we naar publicaties van het European Union Agency for Network and Information Security (ENISA) en het Nationaal Cyber Security Centrum (NCSC).
Voor de beveiligingsmeldingen kun je meer vinden op www.z-cert.nl en www.ecri.org.

[31] *https://www.nvz-ziekenhuizen.nl/onderwerpen/verwerkersovereenkomst*

4.12 | HOE VOORKOM IK EEN DATALEK?

Sinds 1 januari 2016 geldt de meldplicht datalekken. Dit houdt in dat een organisatie zoals het ziekenhuis direct een melding moet doen bij de Autoriteit Persoonsgegevens zodra er een ernstig datalek is.

WAT IS EEN DATALEK?

Een datalek is het ter beschikking komen van data aan daartoe onbevoegde personen, maar ook het kwijtraken van data waardoor deze niet meer beschikbaar zijn. Het gaat dan om tot een persoon herleidbare data, bijvoorbeeld iemands naam, adres, geboortedatum of geslacht, maar ook gezondheidsgegevens en andere bijzondere persoonsgegevens.
De meldplicht datalekken is naast de overige medische informatietechnologie ook van toepassing bij medische apparatuur met medische software. Op een medisch apparaat bevinden zich vaak patiëntgegevens die tot een persoon herleidbaar zijn en deze data mogen niet beschikbaar komen voor ongeautoriseerde personen, tenzij deze data geanonimiseerd zijn. Dit betekent dat een medisch apparaat bijvoorbeeld niet zonder meer mag worden weggegeven, verkocht of weggegooid. De meldplicht datalekken geldt daarnaast ook voor medische software waarin persoonsgegevens verwerkt worden.

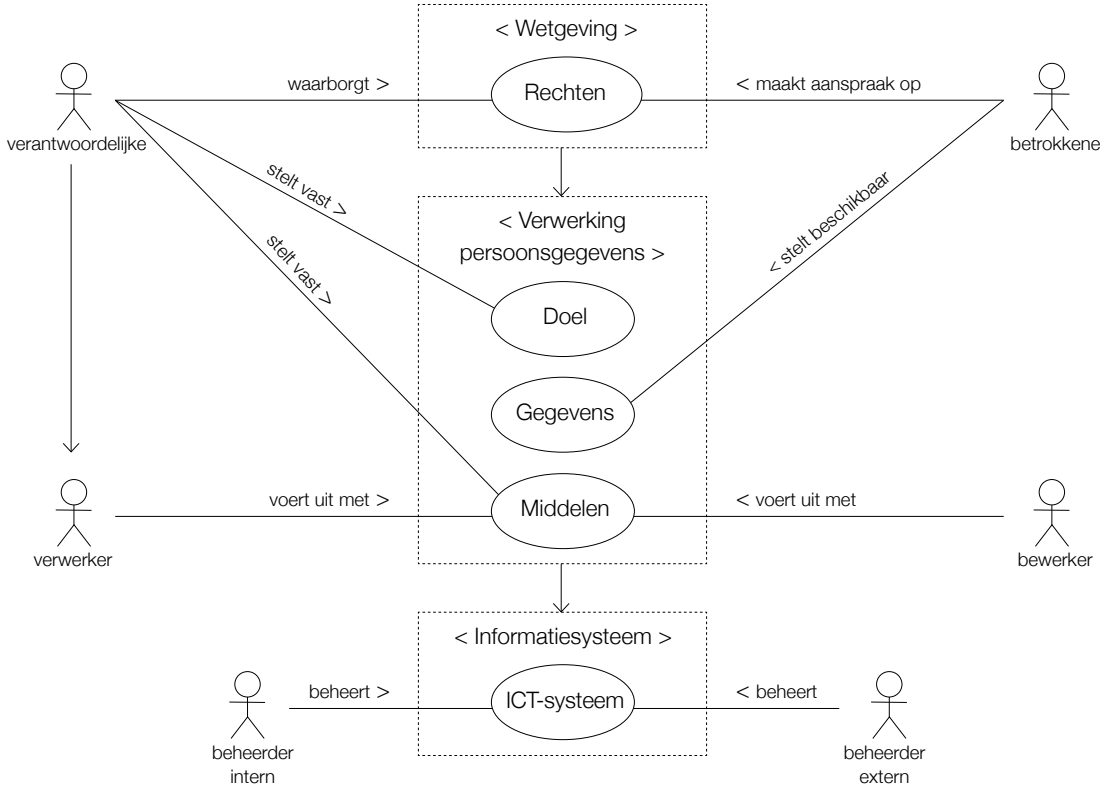
Voorbeelden van mogelijke datalekken:

- niet encrypted usb-stick met patiënt-gegevens kwijtgeraakt in de trein;
- er is een laptop met patiëntgegevens gestolen;
- een telefoongesprek in de trein waarin patiëntgegevens genoemd worden;
- print met patiëntgegevens in een algemene papierpak weggooien of in printer laten liggen;
- verzenden van foto's patiënt via Whatsapp met tot de patiënt herleidbare kenmerken;
- medisch apparaat met patiëntgegevens erop naar ander ziekenhuis overgebracht voor gebruik aldaar;
- het delen van patiëntgegevens met een ziekenhuis zonder dat de betrokkenen onderdeel zijn van het behandelteam van de patiënt;
- het op een onbetrouwbare manier versturen van patiëntgegevens (niet versleuteld);
- een hacker heeft toegang verkregen tot patiëntgegevens;
- een medewerker van de zorginstelling bekijkt de patiëntgegevens van een ziek familielid in het elektronisch patiënten-dossier (epd).

WAT ZIJN DE VERSCHILLENDE ROLLEN IN DE BESCHERMING VAN PERSOONSGEGEVENS?

In de wetgeving is vastgesteld wat de verschillende rollen zijn bij de bescherming van persoonsgegevens. Figuur 4.12.1 geeft dit schematisch weer.
De betrokkene is degene die zijn gegevens beschikbaar stelt en recht heeft op de adequate bescherming van deze gegevens.
De verantwoordelijke is degene die het doel en de middelen van verwerking vaststelt. Het gaat bij zorginstellingen dan om de gehele zorginstelling, niet een individuele medewerker. Als de data alleen verwerkt worden in intern beheer (dus binnen de zorginstelling) dan is er geen verwerker. Een verwerker is iemand die de verantwoordelijke persoonsgegevens verwerkt zonder dat diegene in hiërarchische verhouding staat met de verantwoordelijke. Dit gaat bijvoorbeeld om een leverancier die gegevens verwerkt in opdracht van de verantwoordelijke. Voorbeelden van het verwerken van gegevens is de opslag van gegevens en het uitvoeren van analyses op gegevens voor beslisondersteuning.

TOETSMODEL BESCHERMING PERSOONSGEGEVENS



Figuur 4.12.1 Toetsmodel bescherming persoonsgegevens (Bron: Peter van Hoogdalem, ErasmusMC)

HOE EN WAAR MELD IK EEN DATALEK?

Het ziekenhuis (de verantwoordelijke) heeft de verplichting om zonder onnodige vertraging maar in ieder geval binnen 72 uur een datalek te melden en acties te ondernemen. Het datalek moet gemeld worden bij de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Er is ook vastgesteld wanneer het ziekenhuis de betrokkenen moet informeren over het datalek. Als het goed is, heeft ieder ziekenhuis een procedure opgesteld waarin staat dat een datalek gemeld moet worden bij de Functionaris Gegevensbescherming van de zorginstelling die de procedure verder volgt. Meer informatie over het opstellen van deze procedure staat op de site van de Autoriteit Persoonsgegevens.[32]
Met de invoering van de Algemene verordening gegevensbescherming (AVG), op 25 mei 2018, zijn er strengere eisen aan de registratie van de datalekken. Alle datalekken in de organisatie moeten gedocumenteerd worden, ook de datalekken die niet gemeld (hoeven) worden.

WAT MOET IK REGELEN OM DATALEKKEN TE VOORKOMEN?

Hier benoemen we een aantal zaken die in ieder geval geregeld moeten worden om datalekken, zoals de eerder genoemde voorbeelden, te voorkomen. Het betekent overigens niet dat er geen datalekken kunnen voorkomen als onderstaande maatregelen genomen zijn.
De patiëntgegevens op een medische informatietechnologie of ander medium moeten altijd verwijderd worden bij afvoer van apparatuur. Als de apparatuur niet meer gebruikt wordt, is destructie van de harde schijf de beste optie. Leg vast wie hiervoor verantwoordelijk is, in het geval van een medisch apparaat bijvoorbeeld de verantwoordelijke medisch instrumentatietechnicus. Bij proefplaatsingen van medische apparatuur is het goed om vooraf met de leverancier af te spreken hoe data verwijderd zullen worden omdat de destructie van de harde schijf dan (vaak) niet mogelijk is. Houd er daarnaast rekening mee dat een leverancier bij onderhoud in aanraking komt met deze data, bijvoorbeeld op een echo-apparaat. Indien mogelijk moeten bij onderhoud de data altijd verwijderd worden.
Maak ook afspraken met de leverancier over de geheimhouding van patiëntgegevens.
De WIBAZ/FHI/NEVI SSO (Standaard Service Overeenkomst), artikel 7.6 en de bijlagen Overeenkomst externe verbindingen en Gedragscode, zijn een voorbeeld van vastgestelde afspraken hierover.
Binnen de Europese Unie is het niveau van gegevensbescherming gelijkgetrokken. Dit is echter niet het geval met landen buiten de Europese Unie. Als data de Europese Unie verlaten bij bijvoorbeeld onderhoud en storingsanalyses van een verwerker is het daarom noodzakelijk om extra maatregelen te treffen. Voor Amerikaanse bedrijven is de huidige methode (sinds augustus 2016) om zich te certificeren voor het EU-US Privacy Shield. Voor andere landen of bedrijven die zich niet gecertificeerd hebben, is het noodzakelijk om de privacy te borgen via extra afspraken. De aanbevolen methode is om dit via het Europees modelcontract te regelen (bijlage XIV). [33]
Als de organisatie kiest voor dataopslag buiten het ziekenhuis, kies dan een locatie binnen de Europese Unie om te zorgen dat data onder de juiste regelgeving vallen. Deze landen hebben het juiste privacyniveau ten opzichte van Nederland.

Daarnaast is het altijd vereist om een verwerkersovereenkomst af te sluiten met de leverancier als deze data verwerkt voor het ziekenhuis (en dus verwerker is). Hierin moet onder andere staan dat de leverancier een datalek direct meldt aan het ziekenhuis. Dan kan het ziekenhuis voldoen aan de verplichting om zonder onnodige vertraging maar in ieder geval binnen 72 uur het datalek te melden en actie te ondernemen. Dit betekent ook dat een leverancier die een deel van de databewerking uitbesteedt aan derden, zelf ook met dat bedrijf een verwerkersovereenkomst moet afsluiten.
Als er gegevens tussen zorginstellingen of tussen zorgverleners uitgewisseld worden, kies dan voor een betrouwbare methode. Dit betekent onder andere dat de data versleuteld verstuurd moeten worden en dat de gebruikte sleutel voldoende veilig is. Bekijk ook altijd kritisch of de data wel gedeeld mogen worden met de beoogde ontvanger. Voor individuele patiëntgegevens is het van belang dat er een behandelrelatie geldt tussen de patiënt en de persoon in kwestie of dat het delen van data noodzakelijk is voor de werkzaamheden van die persoon (bijvoorbeeld het delen van informatie tussen arts en medisch secretariaat). Het doel van het delen van de gegevens is dan ten bate van de behandeling van de patiënt. Als voor een behandeling patiëntgegevens met een andere instelling gedeeld worden, moet de patiënt hiervan op de hoogte gesteld worden.
De patiënt moet toestemming verlenen voordat de gegevens worden uitgewisseld, tenzij het om uitwisseling gaat binnen een behandelteam – waaronder ook MultiDisciplinair Overleggen (MDO's) – of het spoed betreft en de patiënt geen toestemming kan geven. Een voorbeeld van het rechtmatig uitwisselen van patiëntgegevens is het, na toestemming van de patiënt, uitwisselen van de medische gegevens bij overdracht van een patiënt naar een ander ziekenhuis voor (een deel van van) zijn behandeling. Denk hierbij bijvoorbeeld aan het versturen van het medisch dossier of diagnostische beeldvorming vanuit het andere ziekenhuis, of het verstrekken van historische gegevens voor een nieuwe behandeling, bijvoorbeeld historische bestralingsgegevens voor een nieuw bestralingsplan.

WAAR KAN IK MEER INFORMATIE VINDEN?

Over de Wet bescherming persoonsgegevens, meldplicht datalekken en Algemene verordening gegevensbescherming is onder andere meer informatie te vinden op www.autoriteitpersoonsgegevens.nl. Voor meer informatie over adequate beveiliging van persoonsgegevens verwijzen we jullie naar het hoofdstuk 4.11 *Wat moet ik doen rondom cybersecurity?* en publicaties van het European Union Agency for Network and Information Security (ENISA) en het Nationaal Cyber Security Centrum (NCSC).

[32] *www.autoriteitpersoonsgegevens.nl*

[33] *Zie bijlage XIV Modelcontractbepalingen op www.mtintegraal.nl.*

4.13 | WAT IS DE GELDENDE WET- EN REGELGEVING BIJ MEDISCHE INFORMATIE-TECHNOLOGIE?

De wet- en regelgeving van medische hulpmiddelen is Europees geregeld met het oog op de vrije handelszone binnen de Europese Unie. Deze wet- en regelgeving wordt door de lidstaten van de Europese Unie overgenomen in de nationale wet- en regelgeving. Medische hulpmiddelen die op de markt worden gebracht moeten, behoudens een tweetal in de wet vastgelegde uitzonderingen, zijn voorzien van een CE-markering. Met deze CE-markering geeft een fabrikant aan dat het product aan de gestelde essentiële eisen in de wet- en regelgeving voldoet en dat de vereiste conformiteitsprocedures zijn gevolgd. Tevens worden er aan de fabrikant eisen gesteld over post market surveillance en vigilance.
In Nederland kennen we de Wet op de medische hulpmiddelen, die is uitgewerkt in een drietal besluiten en daarop gebaseerde richtlijnen, te weten:

- Richtlijn medische hulpmiddelen (93/42/EEG)
- Richtlijn actieve implanteerbare medische hulpmiddelen (90/385/EEG)
- Richtlijn in vitro diagnostiek (98/79/EEG)

In de Wet op de medische hulpmiddelen is vastgelegd dat het gebruik van medische hulpmiddelen die niet als zodanig op de markt zijn gebracht, is verboden. Een dergelijke situatie wordt beschouwd als een economisch delict. Een zorginstelling die in eigen beheer een medisch hulpmiddel maakt, valt niet onder de Wet op de medische hulpmiddelen zolang het dat medische hulpmiddel niet op de markt brengt. Onder het op de markt brengen valt ook het zonder vergoeding ter beschikking stellen aan een andere partij (andere juridische entiteit).
Ook als een zorginstelling zelf een medisch hulpmiddel maakt moet uiteraard aan bepaalde kwaliteitseisen worden voldaan. Formeel zijn hier geen concrete eisen voor opgesteld maar een zorginstelling is wel gehouden aan de Wet kwaliteit, klachten en geschillen zorg (Wkkgz). Deze bepaalt dat een zorgaanbieder zich van zodanige middelen moet bedienen dat deze redelijkerwijs moeten leiden tot het verlenen van goede zorg. Bovendien wordt het ziekenhuis in het kader van de Richtlijn productaansprakelijkheid (Richtlijn 85/374/EEG) in een dergelijke situatie als fabrikant beschouwd en is zij aansprakelijk voor eventuele veiligheidsgebreken.
Het komt er in de praktijk dan ook feitelijk op neer dat een medisch hulpmiddel dat door een zorginstelling wordt gemaakt aan dezelfde essentiële eisen moet voldoen als een medisch hulpmiddel dat door een fabrikant op de markt gebracht wordt. Het medisch hulpmiddel moet dus CE-waardig zijn zonder dat het een CE-markering hoeft te hebben.
De huidige MDD wordt vervangen door de MDR (Medical Device Regulation), er is momenteel sprake van een overgangssituatie.

WAT ZIJN DE BELANGRIJKSTE WIJZIGINGEN BIJ DE OVERGANG VAN MDD NAAR MDR?

In september 2012 is een voorstel gepubliceerd voor een nieuwe Europese Verordening Medische Hulpmiddelen (MDR) om de huidige Medical Device Directive (MDD) te vervangen. In april 2017 heeft het Europese Parlement dit voorstel is aanvaard. Op 26 mei 2017 is de MDR van kracht geworden in alle lidstaten van de Europese Unie en deze MDR moet worden overgenomen in de nationale wet- en regelgeving. In de MDR worden de oude Richtlijn medische hulpmiddelen (93/42/EEG) en de Richtlijn actieve implanteerbare medische hulpmiddelen (90/385/EEG) samengevoegd. Daarnaast is op dezelfde datum de IVDR voor in vitro diagnostiek medische hulpmiddelen van kracht geworden. Er is sprake van een overgangstermijn van drie jaar voor de MDR en van vijf jaar voor de IVDR. Producten die onder de MDD voor 26 mei 2020 op de markt worden gebracht, mogen nog tot 26 mei 2025 worden verkocht. Voor MDR IVD producten is dat 26 mei 2027. Klasse 1 medische hulpmiddelen moeten vanaf 26 mei 2020 (MDR) aan de nieuwe eisen voldoen. De MDR bevat aanvullende en nieuwe eisen voor fabrikanten en Notified Bodies maar ook nieuwe eisen voor zorginstellingen. Zo is in de MDR een bepaling opgenomen omtrent 'home brew medical devices'. Op grond van deze bepaling mogen zorginstellingen onder de MDR alleen nog zelf medische hulpmiddelen maken als deze hulpmiddelen met de vereiste prestatie niet op de markt verkrijgbaar zijn. De zelfgemaakte medische hulpmiddelen moeten voldoen aan general safety and performance requirements; afwijkingen daarvan moeten worden onderbouwd. Daarnaast moet het ontwerp adequaat gedocumenteerd worden (technisch dossier) en moet de instelling over een passend kwaliteitssysteem beschikken.

WELKE NORMEN ZIJN RELEVANT VOOR DE ONDERWERPEN DIE IN PRAKTIJKGIDS AAN BOD KOMEN?

Een fabrikant van een medisch hulpmiddel moet conformiteit met de essentiële eisen uit de richtlijn, de zogenaamde general safety and performance requirements, kunnen aantonen. Voor veel onderwerpen zijn er specifieke geharmoniseerde normen beschikbaar waarvoor geldt dat wanneer conformiteit met de betreffende norm wordt aangetoond, verondersteld wordt dat aan de gestelde essentiële eisen voor dat specifieke onderwerp wordt voldaan. Geharmoniseerde normen zijn normen die door de Europese Commissie zijn gemandateerd. Dergelijke normen krijgen dan de toevoeging EN (Europese Norm). De betreffende norm kent dan in Nederland de toevoeging NEN-EN. Veel geharmoniseerde normen vinden hun oorsprong bij de ISO of de IEC. Zo zijn er duizenden normen op allerlei gebieden voor onder andere medische apparatuur, IT-systemen, IT-netwerken, informatiebeveiliging, kwaliteitssystemen en risicomanagement. Hieronder geven we enkele voorbeelden, waarbij we opmerken dat normen regelmatig gereviseerd worden het dus raadzaam is om de site van de NEN te raadplegen voor de meest recente normen:

- IEC 60601: normenreeks voor medisch-elektrische apparatuur;
- IEC 62304: medical device software development lifecycle;
- ISO 13485: kwaliteitsmanagementsysteem. Eisen voor het ontwerp, fabricage, service en onderhoud van medische hulpmiddelen;
- ISO 9001: kwaliteitsmanagementsysteem;
- ISO 14971: 2012. Toepassing van risico-management bij medische hulpmiddelen.
- IEC/TR 80001: Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities;

- IEC/TR 80002-1 Medical device software – Part 1: Guidance on the application of ISO 14971 to medical device software;
- NEN 7510 Informatiebeveiliging in de zorg.

Naast eisen op het gebied van informatie-beveiliging gelden als, er gegevens worden uitgewisseld, de Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg en de Wet gebruik burgerservicenummer in de zorg. Voor de basis van zorgverlening geldt de Wet op de geneeskundige behandel overeenkomst (WGBO) en ten aanzien van persoonsgegevens en privacy is met ingang van 25 mei 2018 de Algemene verordening gegevensbescherming (AVG) van toepassing. Vanaf die datum geldt dezelfde privacywetgeving in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

Wat verandert er onder meer voor organisaties:
- verwerkingen van persoonsgegevens hoeft niet meer bij de Autoriteit Persoonsgegevens te worden gemeld;
- mogelijk moet er een data protection impact assessment (DPIA) worden uitgevoerd; [34]
- mogelijk moet er een functionaris voor de gegevensbescherming (FG) worden aangesteld.[35]

Op de website van de Autoriteit Persoons-gegevens is meer informatie over de AVG te vinden.[36] Verder kennen we nog diverse richtlijnen, veldnormen en praktische handvatten over de toepassing van medische technologie (in brede zin) die zijn opgesteld door bijvoorbeeld beroepsverenigingen of werkgeversorganisaties, zoals het WINT2.0 rapport van de Koepel Medische Technologie en het Convenant van NVZ, NFU en RN.

WET- EN REGELGEVING BIJ GEÏNTEGREERDE SOFTWARE IN EEN MEDISCH APPARAAT

Software die geïntegreerd is in een apparaat en nodig is voor de werking ervan – de zogenaamde embedded software –, valt onder dezelfde Richtlijn medische hulpmiddelen als het betreffende apparaat. In een van de praktijkvoorbeelden in deze gids, het ECG-apparaat, fietsergometer en de software is dit de 93/42/EEG (met name relevant voor de fabrikant). Relevant voor de zorginstelling zijn: ISO 14971 en de NEN 7510/ ISO 27001.

[34] *https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia?qa=dpia*

[35] *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg*

[36] *https://autoriteitpersoonsgegevens.nl*

WET- EN REGELGEVING BIJ STANDALONE SOFTWARE

Software die valt onder de definitie van een medisch hulpmiddel moet voldoen aan de essentiële eisen uit de betreffende Richtlijn medische hulpmiddelen. Dergelijke software wordt beschouwd als een actief medisch hulpmiddel. Standalone software die gebruikt wordt in de gezondheidszorg kent zeer veel verschijningsvormen. Dit maakt het soms lastig om te beoordelen of bepaalde software al dan niet onder de MDD valt. De Meddev 2.1.6 is een Europese richtlijn bedoeld als ondersteuning bij deze beoordeling. Het IMDRF-document Standalone Medical Device Software heeft een vergelijkbare functie. Heel algemeen gesteld en alleen ter indicatie kun je uit genoemde documenten afleiden dat software die alleen dient voor opslag en transport van data op zich geen medisch hulpmiddel is. Zodra er echter sprake is van een bewerking of interpretatie van data met als doel om daar bijvoorbeeld diagnostiek of therapie mee uit te voeren gaat het meestal om een medisch hulpmiddel.
Het PACS uit het praktijkvoorbeeld valt onder de 93/42/EEG (met name relevant voor de fabrikant). Relevant voor de zorginstelling zijn: ISO 14971 en de NEN 7510/ISO 27001. Wanneer in eigen beheer de software wordt aangepast zijn ook de IEC 62304 en de IEC/TR 80002-1 relevant.

WET- EN REGELGEVING BIJ MEDISCHE SYSTEMEN

Een medisch systeem is de combinatie van een medisch apparaat, niet-medisch apparaat en IT-infrastructuur die samen tot één functioneel geheel worden gevormd.
Als een dergelijk systeem door een fabrikant als één geheel wordt geleverd dan valt dit vanuit de regelgeving onder geïntegreerde software in een medisch apparaat zoals hierboven reeds beschreven. Wanneer een zorginstelling zelf medische apparatuur, niet-medische apparatuur en IT-componenten aan elkaar koppelt, is de zorginstelling zelf verantwoordelijk voor het goed, betrouwbaar en veilig functioneren van het medische systeem.
Het medisch apparaat zelf moet voldoen aan de eisen uit de betreffende Richtlijn 93/42/EEG. Voor de IT-componenten gelden ook specifieke normen waaraan moet worden voldaan zoals de EMC-richtlijn 2014/30/EU.
Het IT-netwerk en het informatiesysteem moeten voldoen aan de NEN 7510/ ISO 27001 norm voor informatiebeveiliging.
Om een goede, betrouwbare en veilige keten te realiseren is een gedegen risicoanalyse een vereiste, daarvoor zijn de ISO 14971 en de ISO 80001 reeks normen en richtlijnen relevant, alsook de IEC 60601-1-8.

WET- EN REGELGEVING BIJ ZELFBOUW VAN SOFTWARE

Voor ontwikkeling van software zijn relevant de IEC 62304, de ISO 14971 en de IEC/TR 80002-1 en ten slotte ook weer de NEN 7510/ ISO 27001.

HET ONDERWERP IS DYNAMISCH, DE PRAKTIJK IS WEERBARSTIG, EN DE WET- EN REGELGEVING IS AAN VERANDERING ONDERHEVIG. HET LAATSTE WOORD OVER MEDISCHE INFORMATIE-TECHNOLOGIE IS ZEKER NIET GEZEGD. WE ZULLEN OP MT-INTEGRAAL BLIJVEN PUBLICEREN EN DISCUSSIËREN OVER HET ONDERWERP EN WE NODIGEN ALLE VAKGENOTEN UIT OM HETZELFDE TE DOEN.

5 | TER DISCUSSIE

Deze Praktijkgids is samengesteld door een aantal deskundigen van verschillende verenigingen uit de Koepel Medische Technologie die regelmatig te maken hebben met beleid en procedures rondom medische informatietechnologie. De gids geeft handvatten om de diverse aspecten in de levenscyclus van medische informatietechnologie goed te regelen. Binnen de groep die de Praktijkgids heeft samengesteld is over diverse onderwerpen gediscussieerd.

Een van de belangrijke discussiepunten was de vraag hoe normatief deze Praktijkgids moet zijn. Zoals we in de inleiding hebben aangegeven willen we nadrukkelijk geen veldnorm beschrijven. We hebben ervoor gekozen om de relevante normen te beschrijven en uit te leggen en van voorbeelden te voorzien. Gezien alle veranderingen waar ons werkveld aan onderhevig is – zoals de overgang van de MDD naar de MDR – is er behoefte aan het beschrijven van de status quo. We hebben niet namens de Koepel Medische Technologie normatief willen optreden en we zijn ook niet in overleg getreden met toezichthoudende instanties om gezamenlijk een standpunt in te nemen.
Uit onze veelvuldige gesprekken en commentaarrondes op elkaars tekst bleek wel dat er genoeg onderwerpen zijn waarover gediscussieerd kan worden. Hoe zit het bijvoorbeeld precies met het delen van zelfgeschreven software? Wat moet je doen als een toepassing buiten de intended use van de producent valt?
De belangrijkste discussiepunten bespreken we in dit hoofdstuk, zonder een panklaar antwoord te geven.

DELEN VAN ZELFGESCHREVEN SOFTWARE

In veel zorginstellingen wordt zelf software geschreven, bijvoorbeeld met Microsoft Excel. Excel wordt regelmatig gebruikt in de zorg, waarbij er in sommige gevallen macro's geschreven worden waarvan het beoogd gebruik valt binnen de definitie van een medisch hulpmiddel. Soms bestaat de wens om een dergelijk bestand te delen met andere zorginstellingen. In veel gevallen is het daarbij niet duidelijk of het dan gaat om een medisch hulpmiddel of niet. Als het gaat om een medisch hulpmiddel mag deze volgens de geldende wetgeving niet gedeeld worden als deze geen CE-markering heeft.
Op dit moment is er een werkgroep vanuit de Koepel op verzoek van de IGJ bezig om richtlijnen vast te stellen voor het gebruik van niet-CE-gemarkeerde hulpmiddelen. Mogelijk brengt dit ook een oplossing voor bovenstaande casus.

IS BESLISSINGSONDERSTEUNING EEN ZELFSTANDIG MEDISCH HULPMIDDEL OF VALT HET BINNEN HET CE VAN HET OORSPRONKELIJKE PAKKET?

Binnen sommige medische software is het mogelijk om regels voor beslissingsondersteuning te schrijven. De vraag is of dit dan weer nieuwe software is of dat dit valt binnen het CE van het oorspronkelijke pakket. In sommige gevallen heeft de leverancier in het beoogd gebruik ook opgenomen dat de zorginstellingen zelf algoritmes voor beslissingsondersteuning kunnen maken. Dit kan betekenen dat het onderdeel uitmaakt van de al aanwezige CE-markering. Dit is een groot verschil met het schrijven van macro's in Excel, waarbij de leverancier dit niet heeft opgenomen in de intended use. In ieder geval moeten ook voor deze regels goede afspraken gemaakt worden over validatie en vrijgave.

VERANTWOORDELIJKHEID VAN HET ZIEKENHUIS BIJ DE VALIDATIE EN HET WIJZIGINGSBEHEER VAN MEDISCHE SOFTWARE

Waar het bij medische apparatuur gebruikelijk is dat het ziekenhuis zelf nog test of het apparaat voldoet aan de gestelde specificaties is dit bij medische software (nog) minder gebruikelijk. Ook het testen van de wijzigingen bij updates en upgrades is niet altijd gebruikelijk. De leverancier is ervoor verantwoordelijk dat bij een update of upgrade de oorspronkelijke CE-markering blijft gehandhaafd; daarvoor kunnen eisen worden opgenomen in koopcontracten en onderhoudscontracten. In dergelijke situaties kan volstaan worden met beperkte tests, uiteraard hangt dat ook samen met de risicoklasse van de betreffende software. Omgekeerd is het bij leveranciers van medische apparatuur met een softwarecomponent minder gebruikelijk om regulier (veiligheids) updates voor de software te leveren, waardoor het kan gebeuren dat er in ziekenhuizen verouderde besturings- en antivirussoftware aanwezig is. Hierdoor zijn systemen kwetsbaarder voor cyberaanvallen.

MOS/MA SYSTEMEN EN DE CLASSIFICATIE HIERVAN

De werkgroep heeft ervoor gekozen om geen stelling voor classificatie (I, IIa/IIb of III) van een MOS/MA-systeem in te nemen. De fabrikant van een medisch hulpmiddel is namelijk op basis van het beoogde wettelijke toepassingsgebied (intended use) verantwoordelijk voor het (juist) uitvoeren van deze classificatie.
Verschillende fabrikanten van MOS/MA-systemen bieden handvatten via white papers, op basis van MDD/MDR, voor de interpretatie en/of hun zienswijze.
Als het ziekenhuis zelf de samensteller van een zogenaamd systeem is geworden en daarmee de fabrikant, dan adviseren wij om de fabrikant/leverancier van eventuele als MH-geclassificeerde deelsystemen (bijvoorbeeld een patiëntmonitoringssysteem met een gateway) deze deelsystemen te laten valideren en eventueel gezamenlijk de gehele keten inclusief de koppeling aan een MOS of MA te valideren. Hiervoor zijn diverse normen beschikbaar zoals de IEC 60601-1-8 en de IEC 80001 reeks. Specifiek voor een alarmsysteem is er de IEC 80001-2-5 (en).

MT-INTEGRAAL

Zoals we hebben laten zien in deze Praktijkgids is er nog veel discussie mogelijk rondom medische informatietechnologie. Het onderwerp is dynamisch, de praktijk is weerbarstig en de wet- en regelgeving is aan verandering onderhevig. Het laatste woord over medische informatietechnologie is zeker niet gezegd. We zullen op MT-Integraal blijven publiceren en discussiëren over het onderwerp en nodigen alle vakgenoten uit om hetzelfde te doen.

6 | GERAADPLEEGDE BRONNEN

- Convenant veilige toepassing medische technologie versie 2.0, onder andere te downloaden van www.igz.nl
- https://www.gov.uk/topic/medicines-medical-devices-blood/medical-devices-regulation-safety
- FDA General Principles of Software Validation. https://www.fda.gov/downloads/MedicalDevices/.../ucm085371.pdf
- IMDRF juni 2013, International Medical Device Regulators Forum NEN-EN-IEC 62304/A1 Medical device software - Software life-cycle processes
- NEN-EN-ISO 14971 Medical devices - Application of risk management to medical devices.
- Medical Device Regulation (MDR): http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32017R0745
- Handreiking Overheid: https://www.rijksoverheid.nl/onderwerpen/medische-hulpmiddelen/documenten/publicaties/2017/12/12/handreiking-medische-hulpmiddelen
- Meddev 2.1/6, jan. 2012 Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices
- SSO versie 3.1 Standaard Service Overeenkomst, te downloaden van www.wibaz.nl
- WINT 2.0 Rapport werkgroep instroom nieuwe technologie, te downloaden van www.wibaz.nl
- Website ZBC Kennisbank Checklist opstellen SLA
- Wikipedia

NORMEN OP HET GEBIED VAN INFORMATIEBEVEILIGING

NEN-ISO/IEC 27001+C11+C1+C2 (nl) Informatietechnologie - Beveiligingstechnieken - Management-systemen voor informatiebeveiliging-Eisen Information technology - Security techniques -Information security management systems - Requirements december 2015.

NEN-ISO/IEC 27002+C1+C2 (nl) Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging december 2015

NEN-ISO/IEC 27005 (en) Information technology - Security techniques - Information security risk management juni 2011

NEN 7510 (nl) Medische informatica – Informatiebeveiliging in de zorg Nederlandse norm oktober 2011.

NORMEN OP HET GEBIED VAN KOPPELING VAN MEDISCHE APPARATUUR AAN IT-NETWERKEN

NEN-EN-IEC 80001-1 (en) Application of risk management for IT-networksincorporating medical devices - Part 1: Roles, responsibilities and activities (IEC 80001-1:2010, IDT) april 2011.

NPR-IEC/TR 80001-2-8 (en) Application of risk management for IT-networksincorporating medical devices - Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2 (IEC/TR 80001-2-8:2016, IDT) mei 2016.

NPR-IEC/TR 80001-2-1 (en) Application of risk management for IT-networks incorporating medical devices - Part 2-1: Stepby-step risk management of medical ITnetworks - Practical applications and examples(IEC/TR 80001-2-1:2012, IDT) juli 2012.

NPR-IEC/TR 80001-2-3 (en) Application of risk management for IT-networksincorporating medical devices - Part 2-3: Guidance for wireless networks (IEC/TR 80001-2-3:2012, IDT) juli 2012.

NPR-IEC/TR 80001-2-5 (en) Application of risk management for IT-networks incorporating medical devices - Part 2-5: Application guidance - Guidance for distributed alarm systems

NPR-ISO/TR 80001-2-6 (en) Toepassing van risicomanagement voor ITnetwerken en medische hulpmiddelen - Deel 2-6: Toepassingsrichtlijn - Richtlijn voor overeenstemming over verantwoordelijkheden (ISO/TR 80001-2-6:2014, IDT).

NPR-ISO/TR 80001-2-7 (en) Toepassing van risicomanagement voor IT -netwerken met medische hulpmiddelen - Toepassingshandleiding - Deel 2-7 : Handleiding voor zorginstellingen om zelf conformiteit metIEC 80001-1 te beoordelen.

NORMEN OP HET GEBIED VAN MEDISCHE APPARATUUR

NEN-EN-IEC 60601 Medical electrical equipment: General requirements for basic safety and essential performance NEN-EN-IEC 60601-1-8: en. Medical electrical equipment - Part 1-8: General requirements for basic safety and essential performance - Collateral Standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems.

7 | LIJST MET BIJLAGES

In de Praktijkgids verwijzen we op sommige plekken naar aparte bijlages die te vinden zijn op de site van MT Integraal. We hebben deze bijlages niet in de gids opgenomen omdat het omvangrijke bestanden zijn. Sommige bestanden zijn afkomstig uit de interne organisatie van een ziekenhuis en zijn dus niet online te vinden.

Bijlage I
Leidraad NIKP: nieuwe interventies in de klinische praktijk

Bijlage II
Standaard overdrachtsformulier

Bijlage III
Medical devices software applications including apps

Bijlage IV
Stappenplan uitgebreide prospectieve risico-inventarisatie (PRI)

Bijlage V
PRI-screening van Jeroen Bosch Ziekenhuis

Bijlage VI
BIV-classificatiemethode van Radboudumc

Bijlage VII
BIA-vragenlijst

Bijlage VIII
TBV-matrix Amphia ziekenhuis

Bijlage IX
BiSL model

Bijlage X
Format van een Pakket van Eisen (PvE)

Bijlage XI
Dossier Afspraken en Procedures (DAP)

Bijlage XII
Checklist Service Level Agreement (SLA)

Bijlage XIII
MDS2-formulier

Bijlage XIV
Modelcontractbepalingen.

COLOFON

Concept, tekst en samenstelling
DEZE UITGAVE IS EEN INITIATIEF VAN DE KOEPEL MEDISCHE TECHNOLOGIE

De werkgroep is samengesteld uit:
HENK IMMING, *VOORZITTER WERKGROEP (VZI)*
JOOST ANSEMS, *UMCU (VZI)*
THIERRY FELKERS, *RADBOUDUMC (NVKI)*
LEO GROENENDAAL, *ERASMUS MC (WIBAZ)*
VERA LAGERBURG, *OLVG (NVKF)*
KOOS VAN RINGELENSTEIN, *UMCG (VZI)*
DAGMAR ROSENBRAND, *LUMC (BMTZ)*
EGON SCHEEPERS, *AMPHIA (NVKF)*
WILCO SCHILLEMANS, *ERASMUS MC (NVKF)*
JANNIS SYNTYCHAKIS, *ISALA (VZI)*
DAVE WAUBEN, *UMCG (NVKFM)*

Redactie
FLOOR JASPERS-GERRITSMA

Grafisch ontwerp en opmaak
KARIN JANSSEN ART&DESIGN