

Resultaat intern onderzoek

STORAGEVRAAG- STUKKEN IN DE ZIEKENHUISSECTOR



ICT in perspectief

M&I/Partners/

adviseurs voor management en informatie

INHOUDSOPGAVE

1	INLEIDING	3
2	BEVINDINGEN	4
2.1	Lineaire autonome groei, sterke groei door projecten	4
2.2	Storage overwegend in eigen beheer	5
2.3	Meer dan 50% opslag is voor beeldinformatie	6
2.4	Trend naar snellere opslagmedia, uitfasering tape	7
2.5	Beperkt aantal fabrikanten domineert de markt	8
2.6	Grote verschillen in bewaartermijnen	10
2.6.1	Archivering en back-up verschillen van elkaar	10
2.6.2	Wettelijke bewaartermijnen	10
2.6.3	Vernietiging	12
2.7	Doorbelasting naar gebruik geen gemeengoed	12
2.8	Wetgeving rondom omslag als complex ervaren	12
2.8.1	Verantwoordelijkheid voor geheimhouding en privacy	12
2.8.2	2.8.2 Eigendomsrecht over de gegevens	13
2.8.3	2.8.3 Privacy versus de USA Patriot Act	13
2.8.4	2.8.4 Goed Beheerd Zorgsysteem (GBZ)	14
2.9	Regierol opslag vooral bij IT-afdeling	14
3	AUTEURS	15



1 INLEIDING

Ziekenhuizen hebben te maken met diverse vraagstukken op het gebied van storage, het opslaan van data. Dit geldt in het bijzonder op het moment dat de storageomgeving vervangen moet worden, of bij projecten die veel opslagcapaciteit vragen. Dit betreft vraagstukken als:

- met welke groei van data moet ik rekening houden;
- houd ik de storageomgeving in eigen beheer of moet ik een vorm van outsourcing toepassen;
- welke technologische ontwikkelingen spelen op het gebied van storagesystemen;
- welke kosten spelen bij vervanging van de storageomgeving;
- moet ik kosten voor storage doorbelasten;
- welke wet- en regelgeving speelt omtrent opslag van data.

Deze vragen vormden de aanleiding voor een onderzoek door M&I/Partners naar de huidige stand van zaken rondom storage binnen ziekenhuizen. Dit document bevat de bevindingen van interviews met een aantal ziekenhuizen en leveranciers, aangevuld met ervaringen uit eerder uitgevoerde storageprojecten (advies, selectie en implementatie).



2 BEVINDINGEN

2.1 LINEAIRE AUTONOME GROEI, STERKE GROEI DOOR PROJECTEN

De groei van de hoeveelheid opgeslagen data is voor alle betrokken ziekenhuizen een belangrijk thema. Als oorzaak van de groei gelden de volgende punten.

- 1 Groeiend aantal bestanden, nieuwe bestandstypen.
Waar in het verleden opslag voornamelijk betrekking had op radiologiebeelden, speelt tegenwoordig de opslag van veel meer typen digitaal beeldmateriaal een rol. Voor het managen van 'niet radiologie' beelden wordt tegenwoordig gebruik gemaakt van tweede generatie PACS ('PACS-2'). Hiernaast spelen ook nieuwe types data een rol: bijvoorbeeld video-opnamen uit de OK of (specifiek in de academische wereld) de opslag van zogenaamde 'DNA-sequences'. Ook vanuit de niet medische wereld is een groeiende behoefte aan opslag, denk hierbij aan beelden van bewakingscamera's.
- 2 Groeiende bestandsomvang van beelden.
Steeds meer geavanceerde modaliteiten produceren beelden met een steeds hogere resolutie. Dit betekent per beeld een grotere bestandsomvang.
- 3 Bestandsuitwisseling met andere instellingen.
Door toenemende mogelijkheden voor het uitwisselen van (beeld)bestanden met andere instellingen groeit het aantal bestanden, omdat met een lokale kopie gewerkt wordt.

De ervaring is dat er sprake is van een lineaire groei van de hoeveelheid data van circa 10% - 20% voor de bestaande systemen (de zogenaamde autonome groei), maar dat de groei meer dan lineair wordt onder invloed van 'projecten' (nieuwe ontwikkelingen). Een project kan dan bijvoorbeeld de introductie van digitale beeldverwerking voor pathologie zijn.

Bij de betrokken ziekenhuizen bedraagt de hoeveelheid opgeslagen centrale data circa 100 tot 200 TB. Uitzondering hierop is het betrokken academische ziekenhuis: daar is de hoeveelheid data een orde hoger. Hier komt nog bij dat bij dit ziekenhuis sprake is van aanvullende, decentrale opslagsystemen, bijvoorbeeld ten behoeve van opslag van onderzoeksgegevens. Op dit gebied speelt gen-onderzoek (genomics) een belangrijke rol. Ter illustratie: een zogenaamde 'sequence' van een menselijk genoom is een bestand met een omvang van circa 2 TB. Om analyses op grote aantallen van deze bestanden uit te voeren, zijn specifieke systemen met eigen opslag beschikbaar. Dit is een voorbeeld van een zogenaamde 'big data' toepassing.

2.2 STORAGE OVERWEGEND IN EIGEN BEHEER

Het merendeel van de betrokken ziekenhuizen heeft de storageoplossing in eigendom en in eigen beheer. Het eerstelijnsbeheer wordt door het ziekenhuis zelf uitgevoerd, voor het tweede/derdelijns beheer (afhankelijk van hoeveel kennis van de storageoplossing in huis beschikbaar is) wordt een beroep gedaan op de leverancier of op een storage-integrator.

Geen van de ziekenhuizen neemt storage af in de vorm van 'clouddienst', bijvoorbeeld voor de opslag van archiefdata of back-up data met lange retentietijden. Aspecten die hierbij meespelen staan hieronder beschreven.

- Privacy-aspect: Ziekenhuizen zijn terughoudend in het plaatsen van gegevens 'buiten de deur' vanwege privacyredenen. Ziekenhuizen houden graag controle over de gegevens vanwege de gevoeligheid van de informatie (patiënt- c.q. medische gegevens). Ook speelt hier de USA Patriot Act: als men al uitbesteden overweegt dan is het zeker niet bij een buitenlandse partij¹.
- Het kostenaspect, waarbij de totale jaarprijs (op basis van pay per use) als hoog ervaren wordt in verhouding tot de aanschafkosten van een 'eigen' oplossing.
- Regievoering: Het feit dat je als ziekenhuis met een 'extra' beheerpartij te maken krijgt.

Toch zien wij een voorzichtige trend van uitbesteden. Verschillende ziekenhuizen hebben bij (recente) vervanging van het opslagsysteem overwogen om de opslag als managed dienst (pay per use) af te nemen. Hoewel de meeste hier niet voor kiezen, is in enkele gevallen een vorm van sourcing toegepast.

- Opslagcapaciteit afnemen op basis van bedrag per GB per maand.
Eén van de ziekenhuizen (een groot, academisch ziekenhuis) neemt storage af in de vorm van een managed dienst (de 'Utility Ready Storage' van HP). Dit is een zogenaamde 'pay per use' oplossing, waarbij op basis van het werkelijke gebruik een overeengekomen bedrag per GB per maand wordt betaald. HP monitort hierbij het feitelijk gebruik en zorgt op basis van een SLA dat tijdig extra opslagcapaciteit beschikbaar gemaakt wordt. Met de uitbreiding zijn dan geen eenmalige kosten gemoeid. De oplossing wordt geleverd in de vorm van apparatuur in het datacenter van het ziekenhuis ('on premise'), niet te verwarren met een oplossing in de 'cloud'.
- PACS inclusief storage als managed dienst, betalen per 'study'.
Twee van de ziekenhuizen nemen hun PACS, inclusief de bijbehorende opslagcapaciteit, af als managed dienst, waarbij een vergoeding per 'study' wordt betaald aan de leverancier. De apparatuur hiervoor staat in het datacenter van het ziekenhuis, waarbij een kopie van de data via een dataverbinding gesynchroniseerd wordt op een externe locatie van de leverancier.

¹ Wat men zich i.h.a. niet realiseert is dat de USA Patriot Act niet alleen voor Amerikaanse leveranciers geldt. Elke partij (dus ook Nederlandse leveranciers) die een belang heeft in de Verenigde Staten is gebonden aan de USA Patriot Act en is verplicht op aanvraag gegevens door te spelen. Van zo'n belang is al sprake wanneer het bedrijf een vestiging in de VS heeft.

We zien echter ook een trend waarbij men afstapt van de geïntegreerde 'alles-in-een' oplossing en juist het PACS gebruik te laten maken van de generieke storage. De PACS servers krijgen dan een share in de storage waarop de PACS zelf zijn opslag en back-up verzorgt. De back-up van de PACS beelden is onderdeel van het PACS.

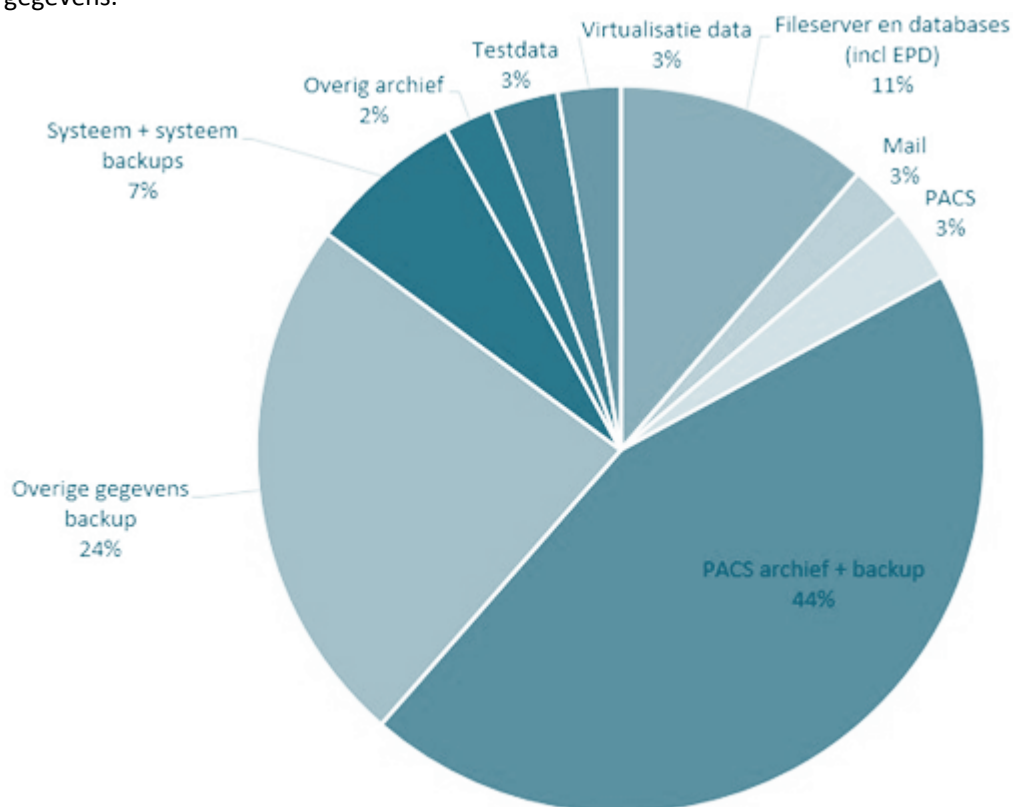
Wat betreft de housing van de storagesystemen geldt bij alle ziekenhuizen dat de data minimaal over twee datacenters verdeeld is. In enkele gevallen wordt de housing van het tweede datacenter van een externe partij afgenomen, waarbij zowel de serversystemen als de storagesystemen in het externe datacenter geplaatst zijn.

2.3 MEER DAN 50% OPSLAG IS VOOR BEELDINFORMATIE

Het overgrote deel van de storagecapaciteit wordt in beslag genomen door beelddata, beeldinformatie die wordt beheerd door het PACS, inclusief archief. Gewoonlijk is dit zo tussen de 50% en 65% van de gebruikte storagecapaciteit. De totale capaciteit van back-upgegevens (inclusief beeldmateriaal) bedraagt gewoonlijk zo rond de 25% - 35%.

Opslag van mail, EPD gegevens en filedata nemen relatief tot de PACS data weinig in beslag.

Daarnaast maken alle ziekenhuizen gebruik van servervirtualisatie en de meeste ook van werkplekvirtualisatie. Een deel van de storagecapaciteit wordt gebruikt voor deze virtualisatie, waarbij het dus niet om gegevensopslag gaat, maar om opslag van sessie- en imagedata. De capaciteit die hiervoor wordt gebruikt, is verwaarloosbaar ten opzichte van de totale hoeveelheid gegevens.



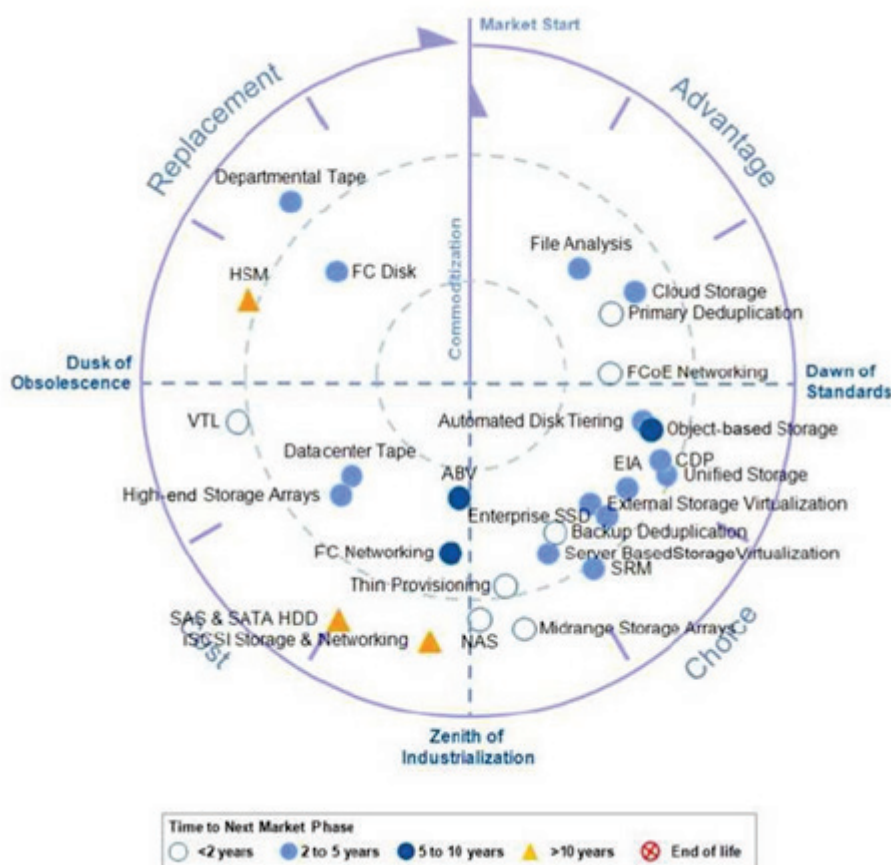
Figuur 1: Voorbeeld van verdeling van capaciteit

2.4 TREND NAAR SNELLERE OPSLAGMEDIA, UITFASERING TAPE

Storagecapaciteit wordt ingedeeld in verschillende 'lagen' (tiers). Er is sprake van snel geheugen waarin gegevens worden opgeslagen die snel (lees: met een zeer lage lees- en schrijfvertraging) beschikbaar moeten zijn (tier 0). De media, die daarvoor worden gebruikt, zijn duur en dus is de capaciteit beperkt. Gegevens die minder snel beschikbaar moeten zijn, worden opgeslagen in tier 1; de totale capaciteit van tier 1 is groter dan die van tier 0, maar de gebruikte opslagmedia is minder snel (en dus goedkoper). Ditzelfde geldt vervolgens ook voor tier 2, enzovoort.

Hoewel nog niet op grote schaal toegepast, worden op tier 0 zogenaamde Solid State Drives (SSD) ingezet. SSD's bevatten geen draaiende onderdelen en zijn bijvoorbeeld gebaseerd op 'flash' geheugen. De SSD storagecapaciteit is in de orde van 1/2% tot 1% van de totale beschikbare storage. SSD wordt vooral ingezet als cache, bijvoorbeeld ten behoeve van werkplekvirtualisatie. Aandachtspunt bij de inzet van SSD is de verwachte levensduur: van een harde schijf is de levensduur gewoonlijk 5 tot 7 jaar, voor een SSD is dit minder duidelijk. Het is bekend dat elk blok van een flash based SSD maar een beperkt aantal malen kan worden overschreven voordat er fouten optreden².

In de praktijk zien wij steeds vaker toepassing van SAS (Serial Attached SCSI) disk technologie in plaats van Fiber Channel disks. Dit sluit aan bij de Gartner Market clock voor storage.

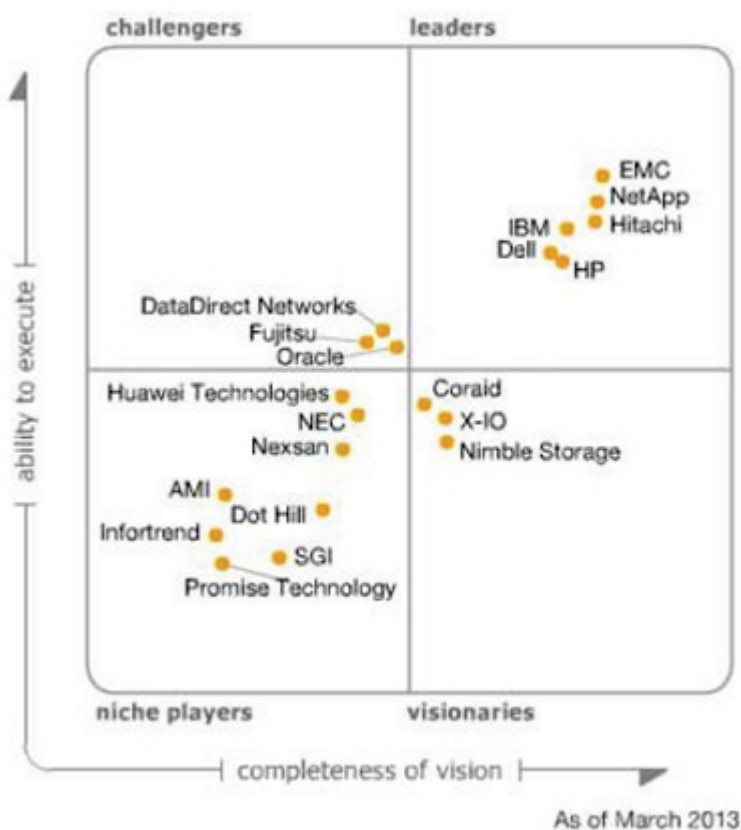


Figuur 2: Storage Market Clock 2012 (bron: Gartner)

Een andere, nog meer prominente trend is de vervanging van tape door diskstorage voor archivering van data.

2.5 BEPERKT AANTAL FABRIKANTEN DOMINEERT DE MARKT

De storageoplossingen, die door de betrokken ziekenhuizen gebruikt worden, zijn van een beperkt aantal fabrikanten: HP, Hitachi, EMC, IBM en NetApp. Al deze partijen staan in het 'leaders quadrant' van de Gartner Magic Quadrant for General-Purpose Disk Arrays (maart 2013).



Figuur 3: Gartner Magic Quadrant for General-Purpose Disk Arrays (maart 2013)

In het magic quadrant zijn zowel midrange systemen als high-end systemen meegenomen, waarbij high-end systemen zich onderscheiden door functionaliteit, capaciteit en performance. In het verleden hanteerde Gartner een verdeling van de storagemarkt op basis van aspecten als architectuur, protocolondersteuning en prijsranges. Het feit dat nu al deze systemen in één overzicht worden opgenomen, illustreert de trend dat zowel qua functionaliteit als qua prijs/performance de midrange systemen en de high-end systemen naar elkaar toegroeien. Gartner verwacht dat dit onderscheid in de komende drie tot vijf jaar in het geheel verdwijnt.

Technische verschillen tussen verschillende storageoplossingen worden kleiner. De kosten voor nieuwe fabrikanten om toe te treden tot de storagemarkt worden steeds lager. Dit komt vooral door de toepassing van standaardcomponenten en het feit dat steeds meer functionaliteit van storage systemen/oplossingen in software worden geïmplementeerd in plaats van in hardware.

- Door de toename van CPU processing power is het ontwerp van storageoplossingen aan het verschuiven van het produceren van specifieke hardwarecomponenten naar het gebruik van standaardcomponenten voor de controllers.
- Veel storagefuncties (zoals snapshot, replicatie, thin provisioning, encryptie, deduplication en RAID) zijn al beschikbaar in standaard filesystems en soms al opgenomen in het operating system of Hypervisor software. Ook zijn ze al los verkoopbaar. Storage vendors zijn in staat om deze software te installeren als softwarepakket op een virtuele host of virtuele storage omgeving. De time-to-market wordt daardoor korter en de kosten lager.

Door de toename van het aantal producten wordt de markt onoverzichtelijker. Vendors proberen marktpositie te behouden en de leading leveranciers houden de markt gesloten. Dit blijkt onder andere uit het volgende:

- kleine verschillen worden disproportioneel door de vendors uitgelicht in hun proposities;
- er zijn afspraken tussen system integrators en fabrikanten over de laagste prijsgarantie;
- Gartner zegt hierover tijdens de 'IT-Infrastructure & Operations Management Summit' van juni 2013.

"The nature of the IT business is that when managing storage a failure or outage is often very severe. Hence, customers live in fear of losing their data and vendors encourage this to charge high margins and spread fear, uncertainty and doubt (FUD) about their competitors. This has led to the market that we have today with a few large vendors, higher margins than other segments of the IT industry and customers who are held hostage by their fear of changing vendor or using new technology".

- Gartner geeft aan dat in sommige contracten opgenomen is dat problemen met storage-systemen niet met derden mogen worden besproken, alleen met de fabrikant van de storageoplossing.

Dit heeft geleid tot een markt waarin een beperkt aantal spelers de markt dicteert met hoge prijzen en hoge marges.

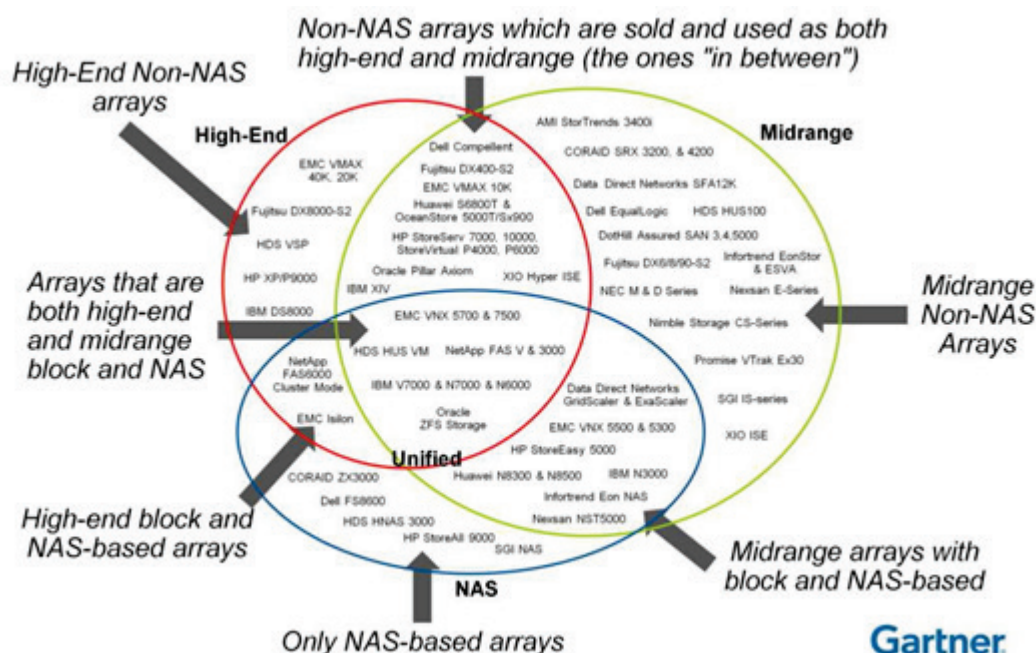
Unified opslag: block- en file based opslag gecombineerd

Het merendeel van de betrokken ziekenhuizen maakt gebruik van een zogenaamd 'unified' storagesysteem. Dit is een storagesysteem dat geschikt is voor zowel de opslag van block-based als file-based gegevens. Het bieden van unified storage is een voorbeeld van high-end en midrange opslagssystemen die in functionaliteit naar elkaar toegroeien.

In de basis bestaat block-based storage uit een hard drive in een server op afstand, welke wordt benaderd met de standaard protocollen Fibre Channel of iSCSI. Block-based storage is zeer flexibel en veelzijdig en is te gebruiken voor vrijwel elk soort applicatie, inclusief file opslag, database opslag, virtual machine file systemen, enzovoort.

File-based storage wordt vaak gebruikt om bestanden tussen gebruikers te delen. De file-based opslag op het centrale storagesysteem is te benaderen via protocollen als NFS (Network File System) en CIFS (Common Internet File System, netwerk file protocol voor bestandsuitwisseling van Microsoft) en vervangt daarmee de traditioneel gebruikte separate NAS-systemen.

Onderstaand figuur van Gartner geeft een overzicht van de modellen per fabrikant, waarbij een verdeling naar high-end, midrange en wel of geen NAS functionaliteit is gemaakt.



Figuur 4: Verdeling storage systemen naar aard

2.6 GROTE VERSCHILLEN IN BEWAARTERMIJNEN

2.6.1 Archivering en back-up verschillen van elkaar

Er is een groot verschil tussen archivering en back-up. Bij een archief gaat het om gegevens die NOOIT meer wijzigen, zogenaamde 'statische data'. Een voorbeeld hiervan is een gemaakte foto van een patiënt. Een back-up slaat een 'momentopname' van gegevens (tijdelijk) op, terwijl het origineel later nog kan wijzigen. Een voorbeeld hiervan is een document waaraan wordt gewerkt: elke dag kan er bijvoorbeeld een back-up worden gemaakt.

Een vraag die bij back-ups speelt, is de retentietijd. Hierbij gaat het om hoe lang een back-up moet worden bewaard zodat gegevens, die bijvoorbeeld onterecht zijn overschreven of weggegooid, weer teruggehaald kunnen worden.

Voor de retentietijden van back-ups is geen wetgeving. Er zijn grote verschillen tussen ziekenhuizen als het gaat om de retentietijden: afhankelijk van de gegevens, tussen een paar weken tot wel 20 jaar. Een vaker toegepast schema is om dagback-ups een week te bewaren, weekback-ups een maand te bewaren, maandback-ups een jaar te bewaren, en dan de jaarback-ups langer te bewaren. De algemene trend lijkt wel dat de retentietijden toenemen.

2.6.2 Wettelijke bewaartermijnen

Op medische gegevens is specifieke wet- en regelgeving van toepassing (o.a. de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) en NEN7510) die eisen stelt aan opslag en bewaartermijnen van deze gegevens. De WGBO kent verschillende bewaartermijnen voor patiënt- dan wel cliëntgegevens. Ook heeft de Wet Bescherming Persoonsgegevens (WBP) richtlijnen voor het bewaren van gegevens.

Volgens de WBP Artikel 10 mag een zorginstelling gegevens niet langer bewaren dan noodzakelijk is voor de doeleinden waarvoor zij worden verzameld en bewaard. Volgens de WGBO en het Burgerlijk Wetboek Boek 7 moeten medische dossiers tien jaar worden bewaard ten behoeve van

wetenschappelijk onderzoek en dergelijke, tenzij de patiënt een verzoek doet om deze informatie te laten verwijderen. Langer bewaren mag alleen, als de zorg van een goed hulpverlener dat vraagt.

Voor de medische dossiers in een academisch ziekenhuis gelden langere bewaartermijnen, tot wel 115 jaar. Niet alle gegevens uit een medisch dossier mogen echter 115 jaar worden bewaard.

Er is veel onduidelijkheid over de lengte van de bewaarplicht. Deze onduidelijkheid wordt mede veroorzaakt doordat definities niet consistent worden gebruikt. Een voorbeeld hiervan is het moment van starten van de bewaartermijn. De WGBO stelt een bewaartermijn van 15 jaar (art. 7:455 BW lid 3), gerekend vanaf het moment dat de gegevens zijn vervaardigd. Daarentegen geldt in andere gevallen dat de termijn start vanaf het moment dat de behandelingsovereenkomst is beëindigd.

Onderstaand overzicht geeft een aantal geldende bewaartermijnen.

- Huisartsenpraktijk.
 - 15 jaar nadat de behandelingsovereenkomst is beëindigd.
 - Langer indien dit 'uit de zorg van goed hulpverlener voortvloeit' (bijvoorbeeld in het geval van erfelijke ziekten).
 - Kinderen langer: 15 jaar nadat ze 19 jaar zijn geworden.
- Langdurige zorginstellingen (zoals VVT instellingen).
 - 7 jaar.
 - In geval dat er ook een verpleeghuisarts is: 15 jaar.
- Jeugdzorg.
 - 15 jaar, maar in ieder geval tot het jongste kind van het gezin ook meerderjarig is.
- Psychiatrisch ziekenhuis.
 - Voor een patiënt die verplicht is opgenomen maximaal 5 jaar.
 - In het algemeen geldt dat een dossier na verloop van deze termijn MOET worden vernietigd.
- Uitslag medische keuring.
 - Zolang noodzakelijk voor het doel van de keuring. In geval van een levensverzekering kan dat dus gedurende de duur van de verzekering zijn.
 - In alle andere gevallen 15 jaar.
- Ziekenhuizen.
 - 15 jaar na afloop behandeling, tenzij uit zorg voortvloeit dat het langer moet zijn.
 - Archiefwet maakt uitzondering voor academische ziekenhuizen.
 - 115 jaar geteld vanaf de geboorte van de patiënt.
 - Geldt alleen voor delen van het dossier (ontslagbrief, anesthesieverslag, PA-verslag, verslag van spoedeisende hulp en bescheiden die gegevens over calamiteiten bevatten).

Hiernaast gelden in bepaalde gevallen afwijkende wettelijke bepalingen. Als een wettelijk voorschrift een andere bewaartermijn noemt, moet die worden aangehouden. Bijvoorbeeld:

- bedrijfsgezondheidszorg stelt dat gegevens uit verplichte medische keuringen in het kader van blootstelling aan gevaarlijke stoffen een bewaartijd kennen van 40 jaar vanaf einde blootstelling (Arbeidsomstandighedenbesluit art. 4.10c);
- besluit patiëntendossier (Bopz) gaat uit van een bewaartermijn van 5 jaar.

Een van de vraagstukken die bij dergelijke bewaartermijnen speelt, is of en hoe de gegevens kunnen worden teruggelezen. De IT-afdelingen van de ziekenhuizen zijn zich bewust van dit vraagstuk, maar houden zich daar niet mee bezig.

Er zijn geen wettelijke termijnen met betrekking tot retentietijden van back-ups.

2.6.3 Vernietiging

Na de wettelijke bewaartermijn moeten de gegevens worden vernietigd. Hiernaast kan de patiënt een verzoek tot vernietiging doen. Hiervoor geldt:

- de gegevens moeten vernietigd zijn binnen drie maanden nadat het verzoek is ingediend;
- uitzondering: wanneer het van belang is voor een ander dat de gegevens bewaard blijven;
- aandachtspunt is dat ook back-ups, archieven, transacties en alle logs daarop moeten worden verwijderd. Dit is niet vanzelfsprekend.

Geen enkel van de door ons ondervraagde ziekenhuizen houdt zich op dit moment bezig met de problematiek rond vernietiging van patiëntgegevens. Dit is vooral omdat dit op dit moment nog niet speelt.

2.7 DOORBELASTING NAAR GEBRUIK GEEN GEMEENGOED

Ziekenhuizen besteden gemiddeld circa 4,3% van het ICT-budget aan storage. Dit betreft de kapitaallasten en de exploitatielasten. (Bron: ICT benchmark Ziekenhuizen 2012, M&I/Partners).

Ziekenhuizen die wij gesproken hebben, belasten storagegebruik nog niet door aan de gebruikers (waaronder de specialisten). Sommige ziekenhuizen belasten wel door aan de afdeling binnen het ziekenhuis, maar nog nergens worden specialisten doorbelast voor het daadwerkelijk gebruik van de storage.

Door de integrale omslag is er ook geen rem op het gebruik van opslag. Een voorbeeld is dat de wetgeving bepaalt dat beelden van specifieke delen van een operatie bewaard moeten blijven. In plaats van dat alleen die beelden worden bewaard, blijft in de praktijk de opname van de gehele operatie bewaard.

2.8 WETGEVING ROND OM OMSLAG ALS COMPLEX ERVAREN

De wetgeving omtrent de opslag van gegevens in ziekenhuizen is complex, soms onduidelijk (hiaten), maar ook hier en daar tegenstrijdig (zie ook paragraaf 2.6.2 over de wettelijke bewaartermijnen). In het algemeen geldt dat ziekenhuizen moeite hebben om de van belang zijnde wetten en regels goed te overzien om alle consequenties te kunnen bepalen.

Wat opvalt, is dat de vakgroepen/specialisten zich weinig betrokken voelen bij dit vraagstuk. Zij laten het vooral over aan de IT-afdeling.

De belangrijkste wetten waaraan moet worden voldaan zijn de Wet Bescherming Persoonsgegevens (WBP) en Wet op de Geneeskundige Behandelingsovereenkomst (WGBO).

2.8.1 Verantwoordelijkheid voor geheimhouding en privacy

WGBO

De WGBO is onderdeel van het Burgerlijk Wetboek. De WGBO regelt toegang tot en beschikbaarheid van het dossier. De WGBO stelt:

- de zorgverlener is verantwoordelijk voor de juistheid en compleetheid van het dossier (art. 7:454 BW – Burgerlijk Wetboek);
- het vernietigingsrecht van het dossier (art. 7:455 lid 1 BW) geeft de patiënt recht het dossier te laten vernietigen en in te zien, maar niet buiten de hulpverlener om;
- inzage- en afschriftrecht (art. 7:456 BW);
- eisen met betrekking op de standaard hoe het dossier moet zijn vormgegeven en opgeslagen (art. 7:453 BW).

WBP

Naast de WGBO is de Wet Bescherming Persoonsgegevens van belang (WBP). De WBP is alleen van belang voor persoonsgegevens (gegevens die te herleiden zijn naar een natuurlijk persoon).

- Art. 21 WBP stelt dat persoonsgegevens door zorgaanbieders alleen mogen worden gebruikt voor het verlenen van zorg of wanneer dit voor het beheer van de zorginstelling nodig is;
- Art. 13 en 14 van het WBP stelt eigenlijk dat aan NEN7510 moet zijn voldaan;
- Art. 13 WBP stelt dat de zorginstelling passende, technische maatregelen neemt om persoonsgegevens te beveiligen tegen verlies of diefstal. En dat maatregelen er op gericht zijn om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen;
- Art. 14 WBP stelt dat als de zorginstelling een derde vraagt de gegevens te verwerken, dat de zorginstelling er zorg voor draagt dat de bewerker voldoende waarborgen biedt ten aanzien van de beveiligingsmaatregelen. Dit is dus van toepassing bij het outsourcen of elders plaatsen van gegevens.

Jurisprudentie

De verantwoordelijkheid voor privacy en toegang tot patiëntgegevens blijft bij de zorgaanbieder, ook als de gegevens elders zijn opgeslagen (outsourcing).

Relevant in deze zijn de volgende artikelen:

- Art. 2 Kwaliteitswet Zorginstellingen (KWZ): zorgaanbieder (in deze de instelling) moet goede zorg verlenen;
- Art. 40 Wet op de Beroepen in de Individuele Gezondheidszorg (BIG): idem, maar nu geldend voor de individuele professional.

Volgens de Inspectie voor de Gezondheidszorg (IGZ) volgt hieruit dat tenminste aan NEN7510 moet zijn voldaan.

2.8.2 Eigendomsrecht over de gegevens

- De wetgeving geeft geen uitsluitsel over het eigenaarschap van de gegevens.
- Volgens jurisprudentie komt beschikking over het origineel van het medisch dossier toe aan de hulpverlener. Of dit de arts of het ziekenhuis is, hangt af van de relatie tussen de arts en het ziekenhuis (dienstverband of arts huurt alleen ziekenhuisruimte).

2.8.3 Privacy versus de USA Patriot Act

De wetswijziging naar aanleiding van de USA Patriot Act geeft de overheid van de VS de mogelijkheid om gegevens van 'in het buitenland verblijvende niet-Amerikanen' op te vragen. Dit is in bepaalde gevallen ook van toepassing op gegevens die niet in de VS staan. Een onderneming valt onder Amerikaanse jurisdictie als het aan het criterium voldoet van 'structureel activiteiten uitvoeren binnen de VS'. Dit is het geval wanneer de onderneming:

- een vestiging in de VS heeft of;
- onderdeel is van een in de VS gevestigde onderneming of;
- data in de VS heeft opgeslagen.

Er is geen mogelijkheid om bevragingen tegen te houden door middel van contractuele waarborgen. De Nederlandse wetgeving met betrekking tot privacy biedt ook geen waarborg. De strenge regels met betrekking tot de USA Patriot Act zijn niet uniek. Er zijn ook andere landen (waaronder Europese landen, met name Zweden en de UK) die vergelijkbare wetten kennen.

2.8.4 2.8.4 Goed Beheerd Zorgsysteem (GBZ)

Voor wat betreft storage geldt dat dit onderdeel is van een zorgsysteem en daarmee onderhavig is aan de eisen die aan een zogenaamd 'Goed Beheerd Zorgsysteem' (GBZ) worden gesteld. Voor de volledigheid is hier een korte beschrijving opgenomen wat een GBZ inhoudt².

In hoofdlijnen gaat het GBZ over techniek, privacy en veiligheid. Het zijn de generieke eisen die worden gesteld aan informatiesystemen om gekoppeld te kunnen worden aan het landelijk schakelpunt (LSP). Het definieert de eisen die worden gesteld aan de beheer- en aan de gebruiksorganisatie en het bevat kwaliteitseisen ('non-functionals') die worden gesteld aan de informatiesystemen. Zo definieert het NICTIZ bijvoorbeeld eisen met betrekking tot authenticatiemiddelen die de zorgsystemen moeten implementeren om daarmee de privacy van de gegevens te waarborgen³. Ook stelt het eisen aan de beschikbaarheid van systemen (minimaal 99,5%), de performance (responsetijden) en capaciteit van de systemen, het in- en uitloggen op applicaties, het loggen van toegang tot applicaties, connectiviteitseisen om de interoperabiliteit tussen alle op de landelijke infrastructuur aangesloten systemen te garanderen, enzovoort.

Voor de kwalificatie van een Goed Beheerd Zorgsysteem (GBZ) wordt uitgegaan van het gegeven, dat iedere zorgaanbieder voldoet aan gestelde wetten, regelgeving en normen. Toezicht en toetsing hiervan blijft belegd bij de daartoe bevoegde toezichthoudende instanties. Een volledige toetsing aan alle eisen uit NEN 7510 vormt momenteel geen onderdeel van de GBZ-kwalificatie. In de praktijk blijkt een aantal concrete eisen voor een GBZ overeen te komen met een deel van de normen uit NEN 7510; daarmee overlappen NEN 7510 en het Programma van eisen GBZ elkaar voor een deel.

2.9 REGIEROL OPSLAG VOORAL BIJ IT-AFDELING

Opvallend is dat de regierol bij storage vooral bij de IT-afdeling ligt. Het gaat niet alleen over de techniek van de oplossing en het beheer daarover, maar vooral ook over bewaartijden, privacyaspecten, enzovoort. En dit terwijl dit vooral een juridisch en vakinhoudelijk vraagstuk is. De specialisten pakken hierin hun rol niet en laten dit vooral over aan IT.

Hier kan een belangrijke rol liggen voor de klinisch fysicus. De klinisch fysicus zou een brugfunctie kunnen vervullen tussen IT en de vakgroepen om te bepalen wat bewaartijden zijn, retentietijden, wie toegang tot welke gegevens mag hebben, enzovoort.

² 3 Bron: http://www.nictiz.nl/uploaded/FILES/html_cabinet/live/Infra/Gedeeld/AORTA_GBx_PvE_Organisatie.htm

³ GBZ definitie stelt hieromtrent

- Dat passen van zorgmedewerkers die zijn voorzien van een bepaald soort certificaten (t.b.v. het controleren van de authenticiteit van de passen) door het zorgsysteem moeten kunnen worden gelezen.
- Paslezers moeten zijn gekoppeld aan werkplekken van gebruikers, zodat alleen geauthenticeerde gebruikers toegang kunnen krijgen tot de zorginformatiesystemen.
- Daarnaast een pincode t.b.v. authenticatie moet worden ingetoetst.

3 AUTEURS



Urs Keller, senior adviseur

Urs heeft een sterk analytisch vermogen en is goed in staat om complexe problemen tot hun essentie terug te brengen. De resultaten van zijn werk hebben een hoog kwaliteitsniveau, hij gaat niet voor 'half werk'. Hierbij houdt hij wel steeds de toegevoegde waarde voor de klant in het oog. In conflictsituaties treedt Urs op als bemiddelaar waarbij hij oog heeft voor de achterliggende belangen van alle partijen.

urs.keller@mxi.nl of 030 – 2 270 500



Richard Sitters, senior adviseur

Richard heeft een sterk analytisch vermogen en is goed in staat de vertaling te maken van de gebruikerswensen en bedrijfsdoelstellingen naar de vereiste proces- en infrastructuuraanpassingen. Met zijn kritisch onderzoekende houding weet hij een probleemstelling vanuit meerdere invalshoeken te benaderen. Daardoor weet hij het echte onderliggende probleem van de klant te identificeren en op te lossen. Richard is resultaatgericht en houdt steeds de toegevoegde waarde in het oog.

Richard.sitters@mxi.nl of 030 – 2 270 500

ICT in perspectief

M&I/Partners/

adviseurs voor management en informatie