Handreiking cameratoezicht in ziekenhuizen

Uitgave van Veiligezorg

StAZ Stichting Arbeidsmarkt Ziekenhuizen

Veiligezorg

Nederlandse Vereniging van Ziekenhuizen

FNV Zorg & Welzijn

CNV Zorg & Welzijn

FBZ vakbond voor zorgprofessionals

NU'91 voor zorgprofessionals

Inhoud

Afkortingen

AP	Autoriteit Persoonsgegevens
Arbowet	Arbeidsomstandighedenwet
AVG	Algemene verordening gegevensbescherming
BW	Burgerlijk Wetboek
DPIA	Data Protection Impact Assessment
FG	Functionaris voor Gegevensbescherming
GEB	Gegevensbeschermingseffectbeoordeling
KNMG	Koninklijke Nederlandse Maatschappij tot bevordering der Geneeskunst
NVZ	Nederlandse vereniging van ziekenhuizen
OR	Ondernemingsraad
PO	Privacy Officer
RDW	Dienst wegverkeer
SEH	Spoedeisende Hulp
SR	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
UMC	Universitair Medisch Centrum
Wet BIG	Wet op de beroepen in de individuele gezondheidszorg
WGBO	Wet op de geneeskundige behandelovereenkomst
WMCZ	Wet medezeggenschap cliënten zorginstellingen
WOR	Wet op de ondernemingsraden
Wpg	Wet politiegegevens
WvSr	Wetboek van Strafrecht

1. Inleiding

Deze handreiking is opgesteld om ziekenhuizen te helpen bij cameratoezicht. Inzet van camera's in ziekenhuizen kan goed zijn voor de veiligheid en voor andere doeleinden. Maar er zitten ook risico's aan de inzet van camera's. Ze leveren een inbreuk op de privacy op en dat weegt in ziekenhuizen zeer zwaar. Daarom moeten ziekenhuizen heel goed nadenken voordat ze cameratoezicht invoeren. Om te helpen bij het maken van de keuzes en om te helpen voldoen aan de juridische eisen is deze handreiking opgesteld.

Cameratoezicht wordt inmiddels in bijna alle ziekenhuizen toegepast voor de beveiliging van gebouwen en medewerkers en hun eigendommen. Er hangen vaak camera's bij de ingang van het ziekenhuis, op de parkeerplaats en in de fietsenstalling. Maar ook binnen de gebouwen neemt het aantal camera's toe. We zien camera's in ontvangsthallen en in veel wachtkamers van de spoedeisende hulp. Maar ook op medische afdelingen neemt het aantal camera's toe: voor monitoring van patiënten, voor toezicht op verwarde patiënten of bijvoorbeeld voor opleidingsdoeleinden. Dat levert vaak vragen op over privacybescherming, techniek en organisatie. Deze handreiking is bedoeld om ziekenhuizen te helpen bij het beantwoorden van die vragen.

Tijd voor een actuele versie

Het is niet voor het eerst dat er een handreiking voor cameratoezicht in ziekenhuizen wordt gepubliceerd. In 2004 publiceerde de NVZ vereniging van ziekenhuizen al een *Handreiking cameratoezicht en beeldopnamen*. In 2009 heeft Veiligezorg een *Handreiking cameratoezicht in ziekenhuizen* gepubliceerd. Die versies zijn inmiddels flink verouderd: de privacywetgeving is ingrijpend veranderd, vooral door de komst van de AVG. Ook de technologie heeft zich verder ontwikkeld. Daarom is er behoefte aan een update. Dat bleek tijdens de regionale overleggen die in het kader van Veiligezorg twee keer per jaar worden georganiseerd. Aan die overleggen doen ziekenhuizen, universitaire medische centra (UMC's), politie en het Openbaar Ministerie (OM) mee. Eén thema komt vaak langs: cameratoezicht. Veiligezorg heeft daarom opdracht gegeven de *Handreiking cameratoezicht in ziekenhuizen* te updaten.

Herkomst informatie

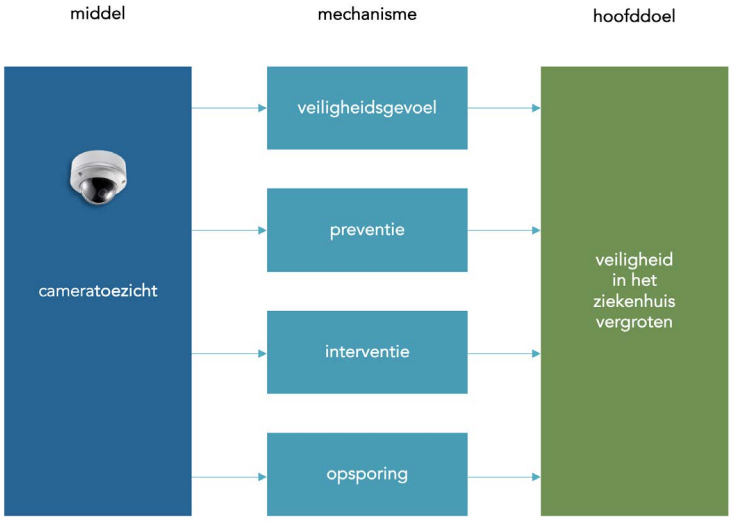
De eerste stap bij het maken van deze handreiking was een inventarisatie van de informatiebehoefte bij ziekenhuizen en hun samenwerkingspartners. Hiertoe zijn gesprekken gevoerd met deskundigen uit tien ziekenhuizen en universitaire medische centra. Ook interne protocollen en reglementen voor camerabewaking zijn opgevraagd en bestudeerd. Daarnaast zijn gesprekken gevoerd met medewerkers van de politie en het OM. Dat leverde een overzicht op van de huidige stand van zaken en van de vragen waar ziekenhuizen, universitaire medische centra, politie en OM antwoord op wilden hebben. Alle informatie is verwerkt in deze handreiking.

2. Camera's in ziekenhuizen

Camera's worden in ziekenhuizen voor verschillende doeleinden ingezet. De bekendste vorm zijn camera's voor bewaking. Dat zijn bijvoorbeeld camera's bij de ingang of in de parkeergarage. Vrijwel elk ziekenhuis heeft dit soort camera's. Maar er zijn ook steeds vaker camera's binnen ziekenhuizen die voor andere doeleinden worden gebruikt, zoals patiëntenzorg of monitoring van verwarde personen. In dit hoofdstuk worden de belangrijkste toepassingen besproken.

2.1 Bewakingscamera's

De bekendste toepassing van cameratoezicht in ziekenhuizen is voor bewaking. Bijna elk ziekenhuis heeft tegenwoordig bewakingscamera's bij de ingang en rondom het gebouw. Ook staan er vaak camera's op parkeerterreinen, in parkeergarages en fietsenstallingen. Dit soort bewakingscamera's zijn meestal bedoeld om beelden op te nemen zodat die gebruikt kunnen worden als bewijsmateriaal. Maar het komt ook voor dat dit soort camera's live worden bekeken. Bewakingscamera's kunnen globaal gesproken op vier manieren bijdragen aan de veiligheid in het ziekenhuis.



Veiligheidsgevoel: een veiliger gevoel bij medewerker, patiënten en bezoekers
Preventie: incidenten worden voorkomen omdat mensen zien dat ze in beeld zijn
Interventie: beveiliger kijkt live mee en kan direct reageren bij incidenten
Opsporing: opnames worden aan de politie verstrekt na een incident

Het is van belang zeer goed na te denken over de doelen die u met bewakingscamera's wilt bereiken voordat u een camerasysteem aanschaft. Voor het opnemen van **bewijsmateriaal** voor opsporing is een camerasysteem nodig dat goede beelden kan maken. De beelden moeten op een veilige en toch gebruiksvriendelijke wijze worden opgeslagen zodat ze als bewijs kunnen worden gebruikt.

Als er nog andere doelen bijkomen, wordt het camerasysteem aanzienlijk ingewikkelder. Stel dat u met camera's een **preventief** effect op daders wilt hebben of het **veiligheidsgevoel** van mensen wilt vergroten. Dan zult u meer moeten doen dan alleen een camerasysteem aanschaffen. Want camera's werken alleen preventief als mogelijke daders *weten* dat er camera's zijn. En mensen krijgen alleen een veiliger gevoel door een camera als ze *zien* dat er camera's zijn. Dat betekent dat u voor deze doelen van cameratoezicht ook zult moeten communiceren over de camera's. De camera's zelf maken deel uit van de communicatiestrategie. De camera's zelf moeten in elk geval goed zichtbaar zijn, evenals de informatiebordjes of -stickers. Daarnaast zult u moeten nadenken over andere manieren om mensen te informeren, want mensen hebben waarschijnlijk meer aandacht voor andere zaken als ze naar het ziekenhuis gaan. Daarbij is het ook van belang heel goed na te denken over de boodschap die het ziekenhuis wil afgeven. Vaak wordt gekozen voor een strenge boodschap die is bedoeld om mogelijke daders af te schrikken: "Let op, u bent in beeld!" Maar wat is het effect van die boodschap op goedwillende mensen? Het is mogelijk dat dit soort communicatie bij hen juist angst aanwakkert: "Er zal hier wel veel aan de hand zijn". Dus voor een veiliger gevoel is een vriendelijke en geruststellende boodschap wellicht beter: "U kunt gerust zijn, want hier is cameratoezicht." Om de juiste toon te treffen en om te zorgen dat uw boodschap mogelijke daders en anderen op de juiste wijze bereikt, is samenwerking nodig met mensen die verstand hebben van communicatie.

Voor live cameratoezicht zijn nog meer investeringen nodig. Want als u de camera's wilt gebruiken om direct te reageren op incidenten ("**interventie**"), dan moeten er niet alleen camera's worden aangeschaft: er moet ook een cameratoezichtruimte worden ingericht en er moeten mensen worden aangenomen en opgeleid die live gaan meekijken. Daarnaast moeten er beveiligers of anderen beschikbaar zijn die heel snel in actie kunnen komen als de observant een incident waarneemt. Daarom vergt live cameratoezicht de meest grondige voorbereiding en aanzienlijke investeringen in tijd, mensen en aandacht van alle camerasystemen.

Kortom: camera's leveren niet alleen technische vraagstukken op (camera's, verbindingen, beeldschermen, opslag, communicatiemiddelen), maar ook organisatorische en juridische vraagstukken (personeel, afspraken, privacy, bewaartermijnen). Camerabewaking lijkt op het eerste gezicht wellicht een vrij recht-toe-recht-aan onderwerp, maar is dat dus zeker niet.

2.2 Camera's voor patiëntenzorg en monitoring

Steeds vaker worden ook camera's ingezet in de patiëntenzorg. Dat was al lange tijd gebruikelijk op de intensive care. Maar het gebeurt nu ook op verpleegafdelingen om herstellende patiënten te monitoren. Of om te waarschuwen als iemand een epileptische aanval krijgt. Of om ouders van pasgeboren kinderen de mogelijkheid te bieden hun kind in de couveuse vanuit huis te zien. De ontwikkelingen gaan snel. Daarom worden hier enkele voorbeelden gegeven die een beeld geven van alle mogelijkheden. Lezers die meer willen weten, kunnen in de bijlage links vinden naar websites met nog veel meer voorbeelden van cameraprojecten in de zorg.

Maastricht UMC+ – Intensive Care
Op de intensive care van het MUMC worden patiënten behandeld, verpleegd en bewaakt met behulp van allerlei apparatuur. Elke éénpersoonskamer is voorzien van een camera waarmee de patiënten kunnen worden geobserveerd. De beelden zijn zichtbaar in de verpleegpost, maar worden niet opgeslagen. Er zijn ook twee kamers op de Cardiovasculaire Care Unit waar patiënten intensieve zorg ontvangen na een hartoperatie of bij acute aandoeningen aan het hart. De camera's zijn verbonden aan een beeldscherm zodat verpleegkundigen de patiënt voortdurend kunnen zien, ook als ze zelf niet in de kamer zijn. Deze beelden worden ook niet bewaard.

Catharina Ziekenhuis – FORSEE
In het Catharina Ziekenhuis in Eindhoven worden hart- of kankerpatiënten die na een ingreep van de intensive care naar een verpleegafdeling gaan niet meer om de zes tot tien uur gecontroleerd op vitale functies. Zij worden 24 uur per dag gemonitord door 'slimme camera's' op de verpleegafdeling: een warmtecamera, infraroodcamera en een omgevingslichtcamera. Deze camera's monitoren de patiënt en kunnen eventuele complicaties direct signaleren. Op die manier kunnen verplegers en artsen eerder ingrijpen, zodat mogelijk levens kunnen worden gered. Bijkomend voordeel is dat patiënten niet om de haverklap wakker hoeven te worden gemaakt. De proef wordt uitgevoerd door artsen en verpleegkundigen van het Catharina Ziekenhuis, in samenwerking met de Technische Universiteit Eindhoven en Fontys Hogescholen. Patiënten moeten eerst toestemming geven vanwege de privacy. En er zit een klepje op de camera waarmee de camera's tijdelijk afgesloten kunnen worden. De proef wordt in 2024 afgerond.

Amphia Ziekenhuis – Braincare
In Breda in het Amphia Ziekenhuis hangen camera's bij de afdeling Braincare. De artsen willen via de camera kunnen meekijken hoe het gaat met een patiënt, bijvoorbeeld om te zien of iemand een epileptische aanval krijgt. Het gaat dus om 'medisch monitoren'. De camera's zijn geplaatst in de eenpersoonskamers en ze staan niet continu aan. Ze gaan bijvoorbeeld uit als er een medewerker op de kamer is. De beelden worden ook niet opgenomen. Patiënten worden geïnformeerd over het feit dat er camera's worden ingezet en mogen dit weigeren als ze er bezwaar tegen hebben. De techniek die nodig was voor dit camerasysteem werd door de technisch beheerder van het ziekenhuis gerealiseerd. De juridische aspecten werden door de jurist van het ziekenhuis geregeld. Een wens van het ziekenhuis is om in de toekomst ook beelden op te nemen zodat de zorg nog meer kan worden verbeterd. De beelden zouden dan onderdeel moeten worden van het elektronisch patiëntendossier (EPD). Dat heeft als voordeel dat de informatie kan worden gebruikt voor betere zorg.

En tegelijkertijd wordt hierdoor geregeld dat de informatie alleen toegankelijk is voor geautoriseerde functionarissen, zoals artsen, medisch specialisten, verpleegkundigen en psychiaters.

Ommelander Ziekenhuis – BabyBeeld
Pasgeboren baby's die nog niet meteen naar huis mogen worden in het ziekenhuis verzorgd – meestal op de couveuseafdeling. Ouders kunnen hun kindje in het Ommelander Ziekenhuis in Groningen dankzij BabyBeeld op elk moment van de dag zien op het scherm van hun smartphone, tablet of computer. Er wordt een camera opgehangen boven de couveuse of het wiegje en dat gebeurt volgens de wensen van de ouders: soms de hele baby in beeld, soms vooral het gezichtje. Het systeem is beveiligd: de ouders bepalen wie de camerabeelden mogen zien: het ziekenhuis geeft ze een persoonlijke inlogcode. De camera's geven uitsluitend beelden door en geen geluid. Ook worden de beelden niet opgenomen. De verpleegkundigen zijn enthousiast over het systeem, vooral over de eenvoud van de installatie en het gebruik.

2.3 Andere camera's

Naast de hier besproken camerasystemen zijn er in ziekenhuizen nog veel meer camera's. Bijna alle medewerkers, patiënten en bezoekers hebben immers een smartphone bij zich waarmee ze opnames kunnen maken. Daarnaast zijn er in de zorg specialistische toepassingen van camera's, bijvoorbeeld bij kijkoperaties, videoconsulten en dergelijke. Ook zijn er ziekenhuizen die een camera hebben in een ruimte waar een persoon verblijft die een vrijheidsbeperkende maatregel opgelegd heeft gekregen. Deze handreiking gaat alleen over de meer grootschalige camerasystemen die hierboven zijn beschreven. Lezers die meer willen weten over specifieke camera's in ziekenhuizen kunnen terecht op een van de websites die in de bijlage staan. Overigens is het wel verstandig om in het camerabeleid van het ziekenhuis ook aandacht te besteden aan alle andere camera's. Want de wet- en regelgeving is ook op die andere camera's van toepassing. En ook bij het bouwen en beheren van camerasystemen kan een integrale benadering goed uitpakken: één centrale en gecoördineerde opslag voor alle camerabeelden in het ziekenhuis is bijvoorbeeld veel beter te beheren en te beveiligen dan allemaal aparte kleinschalige opslagmedia. Ook de communicatie (stickers, informatiebordjes, webpagina's) over de camera's is effectiever en efficiënter als die over alle camera's in het ziekenhuis gaat.

3. Technologie

In dit hoofdstuk gaat het over de techniek van cameratoezicht. We gaan in op de camera's zelf, maar ook op de andere onderdelen van een camerasysteem, zoals de verbindingen, opslag en software. Cameratechniek is ingewikkeld en vereist specialistische vakkennis. Daarom is het raadzaam u goed te laten informeren door een leverancier of een onafhankelijk technisch adviseur. In dit hoofdstuk worden de belangrijkste principes besproken en worden enkele fundamentele keuzes beschreven.

3.1 Camera's

Camera's zijn er in alle soorten en maten. Er zijn camera's te koop voor minder dan honderd euro en er zijn camera's die tienduizenden euro's per stuk kosten. De kosten zijn onder andere afhankelijk van het aantal pixels, maar ook van de lens, de grootte van de beeldsensor en de lichtgevoeligheid. Het is van belang goed na te denken over het doel van de camera en daar rekening mee te houden bij het kiezen van een camera. Ook de plek van de camera is van belang. Als een camera de openbare ruimte moet filmen, zal een camera nodig zijn die goed kan omgaan met verschillende lichtomstandigheden: van zeer fel licht tot diepe duisternis. Een camera die binnen wordt opgehangen brengt meestal plekken in beeld waar de lichtomstandigheden minder variabel zijn. Dat is eenvoudiger om goed in beeld te brengen. Maar dat geldt natuurlijk niet als het licht op die plek soms aan is en soms uit. Zo zijn er nog meer factoren om rekening mee te houden; enkele belangrijke worden hieronder besproken.

Vast en draaibaar

Een belangrijk verschil tussen soorten camera's is hun beweegbaarheid. Sommige camera's staan altijd op hetzelfde punt gericht, bijvoorbeeld op een slagboom of nooduitgang. Deze vaste camera's worden ook wel staafcamera's genoemd. Er zijn daarnaast ook camera's die kunnen draaien en inzoomen: de pan-tilt-zoom (PTZ) camera's. Meestal worden die camera's gemonteerd in een ronde, koepelvormige behuizing en daarom worden ze ook wel domecamera's genoemd. Er zijn ook ondoorzichtige behuizingen te koop: dan kan een voorbijganger niet zien welke kant de camera op is gericht. Vaste camera's hebben het voordeel dat ze zo worden ingesteld dat ze altijd een perfect plaatje opleveren voor de plek die ze in beeld moeten brengen. Draaibare camera's hebben als voordeel dat ze kunnen worden gericht op incidenten, waardoor er minder camera's nodig zijn om een gebouw of groter terrein helemaal in beeld te krijgen. Het hangt van uw doel en werkwijze af welke variant het meest geschikt is.

Figuur 3.1 Een vaste camera en een dome camera

360-graden camera's

Een camera brengt altijd maar één plek in beeld. Een PTZ-camera kan wel draaien, maar ook die mist altijd alles wat 'achter de rug' gebeurt. Daarom zijn er 360-graden camera's ontwikkeld. In één behuizing worden dan twee of meer camera's gemonteerd die samen alles filmen. Op die manier wordt er nooit iets gemist omdat het buiten beeld gebeurde. Er zijn ook combinaties mogelijk: een ring van vier camera's die continu een overzichtsbeeld bieden met daaronder een bedienbare camera die kan inzoomen. Deze gecombineerde camera's zijn uiteraard duurder dan enkelvoudige camera's. Maar dat is niet het enige: ze produceren ook nog eens vijf keer zoveel beeld per camerapositie als een reguliere camera. Dus is er ook vijf keer zoveel bandbreedte en opslagruimte nodig. En als de beelden live worden bekeken, zijn er ook vijf beeldschermen nodig. Denk daarom vooraf goed na over de vraag hoe belangrijk het is om voortdurend een totaalbeeld te hebben. In de meeste ziekenhuizen worden dit soort gecombineerde camera's alleen opgehangen op plekken waar voortdurend veel mensen zijn, zoals in de ontvangsthal.

Figuur 3.2 Meerdere camera's in één behuizing

Bodycams

Bodycams zijn kleine, draagbare camera's die op het lichaam worden gedragen. Er zijn ziekenhuizen in Nederland waar de beveiligers een bodycam dragen voor hun eigen veiligheid. Juridisch gezien is het ook mogelijk ander personeel een bodycam te geven: in het buitenland gebeurt dat al in bepaalde typen zorg, bijvoorbeeld op gesloten afdelingen waar psychiatrische zorg wordt geboden. Voor zover bekend is dat in Nederlandse ziekenhuizen nog niet het geval en zijn beveiligers de enige met een bodycam.

Bodycams zijn meestal uitsluitend bedoeld voor het tegengaan van agressie en geweld. Het idee is dat bodycams ervoor zorgen dat patiënten en bezoekers minder agressief of gewelddadig zullen zijn omdat ze zich realiseren dat ze worden gefilmd. Ook beveiligers zelf zijn zich bewust van de bodycam en zullen daardoor meer de-escalerend optreden, is de gedachte. De juridische grondslag volgt uit de doelstelling: de bodycams worden uitgereikt door de werkgever op grond van Arbowet en het Burgerlijk Wetboek. Daarin worden werkgevers verplicht een veilige werkplek te bieden. Uiteraard moeten de beelden goed worden beveiligd en alleen worden getoond aan geautoriseerde functionarissen of opsporingsambtenaren. In de bijlage staat een link naar een handreiking voor de inzet van bodycams in ziekenhuizen.

Figuur 3.3 Bodycams

Ziekenhuizen kunnen zich afvragen of bodycams wel zijn toegestaan aangezien er een medisch beroepsgeheim geldt. Dat hangt af van een aantal verschillende factoren – net als bij andere camera's in ziekenhuizen. Het juridische hoofdstuk in deze handreiking gaat daar nader op in. In ziekenhuizen komt daarnaast ook nog een ethische afweging in beeld bij bodycams. Bodycams gaan immers veel verder dan andere camera's. Een standaard bewakingscamera neemt alleen beeld op, maar een bodycam neemt ook geluid op. Dat is dus een grotere inbreuk op de privacy. En bodycams worden op de borst gedragen, waardoor ze veel meer opvallen dan reguliere camera's. Dat is de bedoeling, maar het gaat qua privacy schending veel verder dan een reguliere bewakingscamera. Overigens spelen leveranciers van bodycams inmiddels in op de vraag vanuit de zorg. In plaats van de grote bodycams die beveiligers en politiemensen dragen, worden kleinere bodycams gemaakt speciaal voor zorginstellingen, zoals hierboven te zien is. De afweging of het wenselijk is om met bodycams te gaan werken in het ziekenhuis, moet dan ook worden gemaakt door het hogere management.

Drones

Sommige ziekenhuizen willen met behulp van drones toezicht houden: dat levert tijdwinst op omdat beveiligers dan niet zelf fysiek een ronde hoeven te maken over het terrein. Daarnaast kunnen drones op plekken komen waar mensen maar moeilijk kunnen komen. Maar het blijkt niet eenvoudig om drones in te zetten: de ziekenhuizen die dit hebben onderzocht liepen tegen veel barrières en risico's aan. Deels volgen die uit de privacywetgeving: het is voor een ziekenhuis in principe niet toegestaan de openbare weg in beeld te brengen. Drones doen dat al vrij snel en dat levert dan een grotere inbreuk op de privacy op dan proportioneel is.

Daarnaast gelden voor drones ook luchtvaartregels: het is niet zonder meer toegestaan met een drone te vliegen. Sinds 2020 moeten exploitanten van drones zich registreren bij de RDW. Voor speelgoeddrones is een uitzondering gemaakt: daar is geen vliegbewijs voor nodig. Maar voor professioneel gebruik van een drone is wel een bewijs nodig. In bepaalde gebieden is zelfs een vluchtvergunning vereist van de Inspectie Leefomgeving en Transport, zoals in de buurt van vliegvelden of militaire terreinen. Inzet van drones is op zich wel mogelijk – ook juridisch – maar het kost zoveel tijd en moeite voor een ziekenhuis om een drone in te mogen zetten, dat dit meestal niet opweegt tegen de (vaak kleine) efficiencywinst.

3.2 Opslag, verbindingen en videomanagement

Camera's worden beheerd en bekeken met behulp van een videomanagement-systeem. Daar zijn allerlei varianten van. Twee grote merken zijn Genetec en Milestone, maar veel leveranciers hebben hun eigen specifieke systeem. Van belang is dat het videomanagementsysteem goed wordt beveiligd en wordt ingericht. Ook moeten er regelmatig updates worden doorgevoerd, zoals security updates.

Kwaliteitssystemen en certificering

Er zijn ISO-certificaten voor videosystemen en informatiebeveiliging die bij de selectie van een cameraleverancier als eis kunnen worden opgenomen in de aanbesteding. Het is daarnaast raadzaam in het contract met de leverancier op te nemen dat er een jaarlijkse kwaliteitscontrole wordt uitgevoerd om te zien of alle camera's, verbindingen, software en hardware nog functioneren. Laat daar jaarlijks een voortgangsrapportage over opstellen, zodat eventuele gebreken tijdig aan het licht komen. Ook is het wenselijk om van leveranciers te vragen een jaarlijks verslag te leveren over de informatiebeveiliging. Deze afspraken kunnen worden vastgelegd in een verwerkersovereenkomst –een privacy officer kan daarbij helpen. Voor de inhoudelijke technische details is hulp van de afdeling ICT of automatisering nodig: zij helpen ook bij het opstellen van het Programma van Eisen dat voor aanbestedingen wordt gebruikt en bij het beoordelen van de offertes.

Cloud

Tot op heden worden camerabeelden in ziekenhuizen nog meestal op het eigen lokale netwerk opgeslagen. Opslag van data in de cloud is voor sommige ziekenhuizen nog een stap te ver omdat ze volledige controle willen hebben over de vaak gevoelige informatie die ze verwerken. Maar er zijn ook ziekenhuizen die wel werken met opslag van data in de cloud. In elk geval is duidelijk dat opslag van data in (private) cloudomgevingen steeds populairder wordt. Daar is ook reden toe. Hoewel de beveiliging van data in de cloud inderdaad een uitdaging is, realiseren velen zich dat er ook nadelen en risico's zitten aan lokale opslag van data. Lokale opslag is bijvoorbeeld veel gevoeliger voor brand, waterschade of storingen dan de cloud.

Werken in de cloud biedt ook specifieke voordelen op het gebied van camera's. Ten eerste is het eenvoudiger voor leveranciers om updates van de software door te voeren in uw systeem. Security patches kunnen direct worden geïnstalleerd zodra ze beschikbaar zijn waardoor het risico op een datalek of hackers veel kleiner wordt. Ten tweede is het veel eenvoudiger, maar ook veiliger en juridisch beter onderbouwd om camerabeelden aan de politie te verstrekken via een beveiligde link naar een online opslag in plaats van op een USB-stick of andere externe gegevensdrager. Het is onmogelijk de regie te voeren over een kopie die op een externe gegevensdrager is geleverd. Door de politie online toegang te geven tot het bronbestand worden alle bewerkingen met de opnames automatisch gelogd. Dat maakt het mogelijk om bij te houden wat er precies met elke cameraopname is gebeurd, zoals wie er op welk moment naar de beelden heeft gekeken. Elk ziekenhuis moet hier een eigen afweging in maken: sluit met uw cameraplan in elk geval aan bij het beleid voor informatiebeveiliging dat geldt voor uw ziekenhuis.

3.3 Nieuwe software: slimme camera's

Cameratoezicht is niet goedkoop: de hardware, software en verbindingen kosten geld. Maar ook personeel is tijd kwijt aan cameratoezicht: voor het live bekijken van de camerabeelden of het doorzoeken van opnames om relevante fragmenten terug te vinden. Om die personele kosten te reduceren wordt op allerlei manieren geprobeerd camera's "slimmer" te maken – met wisselend succes. Er is software op de markt van leveranciers die claimen dat ze op basis van kunstmatige intelligentie kunnen helpen bepaalde typen incidenten (agressie, vallende personen) op te merken en deze door te geven aan een medewerker. Ook is het mogelijk alle opgenomen beelden te indexeren en van tekst labels te voorzien, zodat het vinden van een specifieke gebeurtenis sneller gaat.

Toevoegen van extra zintuigen aan camera's

Intelligent cameratoezicht kan ook op een andere manier worden gerealiseerd: door de camera's zelf slimmer te maken door er bijvoorbeeld een microfoon naast te installeren die geluiden kan analyseren en op die manier agressie, brekend glas of hulpgeroep kan herkennen. Of een infraroodlens die ook bij

duisternis en slecht weer bruikbare beelden kan maken. Of een warmtesensor die kan ‘zien’ of ergens personen zijn of niet. In gecontroleerde omstandigheden werken dit soort extra toevoegingen vaak redelijk goed, maar in situaties met veel wisselingen in licht en geluid (dus buiten het ziekenhuis) leveren de systemen vaak erg veel valse alarmen op.

Valse alarmen

De meeste “slimme” camerasystemen zijn nog niet zo slim als de eindgebruikers graag zouden willen. De innovaties volgen elkaar snel op, maar de resultaten vallen vaak nog tegen. Dat heeft een aantal oorzaken. Eén van de belangrijkste drempels is de enorme hoeveelheid informatie die door camera’s wordt geproduceerd. Als in een ziekenhuis vijftig camera’s hangen die allemaal 25 beelden per seconde produceren, moeten er dus 1.250 beelden per seconde worden beoordeeld door de computer. Er zijn nauwelijks computers die dat aankunnen. Daarom wordt gezocht naar manieren om de *information overload* te voorkomen. De beelden worden bijvoorbeeld gecomprimeerd, maar daardoor gaat andere – soms essentiële – informatie verloren.

Een tweede probleem is dat de meeste slimme camera’s wel alarmen genereren, maar ook veel valse alarmen. Om de software te trainen in het juist onderscheiden van relevante informatie en ruis is vaak per camera veel tijd nodig om alles juist in te stellen. Dat kost soms zo veel tijd dat het aantal valse alarmen lange tijd hoog blijft wat er uiteindelijk toe leidt dat de eindgebruikers het systeem uitschakelen en er niet meer mee willen werken. Het is daarom belangrijk altijd eerst een proefopstelling te testen en voldoende tijd te reserveren voor het inregelen van de software.

Anonimiseren of blurren

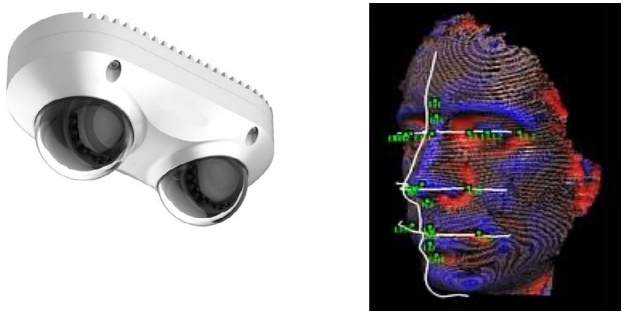
Het is mogelijk camerabeelden te ‘blurren’ door gezichten en kentekens onherkenbaar te maken. Dat kan zowel direct bij de camera gebeuren als achteraf. Anonimisering heeft een positief effect op de privacy. Maar ook na blurren kunnen mensen soms toch nog herkenbaar zijn, denk aan kleding, sieraden, tatoeages. Blurren heeft enkele nadelen. Ten eerste is het juist de bedoeling mensen te kunnen herkennen op camerabeelden, zoals bij opsporingsonderzoek. Ten tweede levert blurren vaak vragen op over de authenticiteit van beeldmateriaal waardoor de juridische bruikbaarheid ter discussie staat. Dat laatste punt komt in het volgende hoofdstuk aan bod. In elk geval is er geen eenduidig antwoord op de vraag of blurren altijd een goed idee is of niet: het hangt af van het doel van uw camerasysteem en de afweging tussen privacybescherming en andere belangrijke doeleinden.

Gezichtsherkenning

Automatische gezichtsherkenning met camera’s werkt steeds beter, maar er zitten technische en juridische haken en ogen aan. Bij gezichtsherkenning is het allereerst van belang onderscheid te maken tussen verificatie en identificatie. Van verificatie is sprake bij bijvoorbeeld toegangscontrole: de biometrie van het gezicht van de persoon die voor de camera staat wordt vergeleken met de biometrische informatie in een pasje of in een paspoort. Of het gezicht dat de smartphone of laptop ziet wordt vergeleken met het opgeslagen gezicht van de eigenaar van de smartphone of laptop. Dat is dus een één-op-één controle. Identificatie daarentegen werkt heel anders: dit wordt ook wel gezichtsherkenning ‘in het wild’ genoemd. Bij identificatie gaat het om het herkennen van een individu uit een database met vergelijkingsmateriaal. Soms zitten er miljoenen of zelfs miljarden foto’s in zo’n database. Dat is een één-op-veel identificatie. Toegangscontrole met behulp van verificatie werkt veel beter dan identificatie – vooral onder gecontroleerde omstandigheden en met subjecten die herkend willen worden. Denk aan de toegangscontrole in een gebouw of het ontgrendelen van een smartphone met je gezicht.

Identificatie daarentegen werkt veel minder goed om een aantal redenen. Ten eerste omdat het voor computers heel moeilijk is om te bepalen waar de gezichten in een camerabeeld zitten. Detectie van gezichten is nog altijd een grote uitdaging in camerabeelden ‘in het wild’. Ten tweede is het voor een computer – die immers een tweedimensionaal beeld analyseert – onmogelijk om diepte te zien. Dus kan een computer niet vaststellen of iemand een smal gezicht heeft of zijn hoofd schuin houdt. Ten derde is er het probleem van occlusie: gezichten zijn soms maar voor de helft zichtbaar, bijvoorbeeld omdat mensen achter elkaar staan of door een zonnebril, hoofddeksel of slechte verlichting. Bij verificatie spelen al die problemen geen rol, omdat mensen hun gezicht recht voor de camera houden en goed worden belicht. Er wordt hard

gewerkt aan het optimaliseren van identificatie, bijvoorbeeld door gebruik te maken van stereocamera's die diepte kunnen zien.



Figuur 3.4 Met een stereocamera kan diepte worden gezien

Maar er is bij identificatie een fundamenteel probleem dat nauwelijks oplosbaar is: personen kunnen alleen worden geïdentificeerd als er een bestand is met biometrische gezichtsinformatie om de camerabeelden mee te vergelijken. Voor de medewerkers van een ziekenhuis kan zo'n personeelbestand nog wel worden gemaakt, maar niet voor alle mogelijke patiënten en bezoekers. Zelfs als het lukt om iemands gezicht in beeld te krijgen blijft het de vraag wie die persoon is. Er zijn bedrijven, zoals Clearview AI, die claimen dat hun software voor gezichtsherkenning bijna iedereen kan herkennen. Die bedrijven vulden hun databases echter zonder toestemming van de betrokkenen door publieke websites zoals Facebook en LinkedIn te 'scrapen'. Ze kopieerden alle foto's van die websites, voegden de naam aan de foto toe en componeerden zo een unieke biometrische 'vingerafdruk' van elk gezicht. Die vingerafdruk kunnen ze vervolgens gebruiken om in nieuwe camerabeelden willekeurige mensen te herkennen. Maar het is niet toegestaan dergelijke databases op te bouwen zonder toestemming van de personen waar het over gaat. Daarom heeft Clearview AI boetes van tientallen miljoenen euro's opgelegd gekregen van onder andere de Italiaanse en Franse nationale privacy toezichthouders. In 2024 heeft Europa de verordening voor kunstmatige intelligentie, de AI-act, aangenomen. Daarin is automatische gezichtsherkenning in publieke ruimten zelfs helemaal verboden ('real-time massasurveillance met gebruik van biometrische gegevens'). De enige uitzondering is gemaakt voor veiligheidsdiensten als die zoeken naar verdachten van een ernstig misdrijf of slachtoffers van bijvoorbeeld een ontvoering. Kortom: verificatie van personen op basis van gezichtsherkenning voor bijvoorbeeld toegangscontrole is mogelijk. Maar identificatie van willekeurige personen 'in het wild' zal voor ziekenhuizen in verreweg de meeste gevallen geen optie zijn – zelfs als het goed zou werken is het in de meeste gevallen niet toegestaan.

3.4 Zelf doen of uitbesteden?

Dit hoofdstuk gaat over cameratechniek en biedt de belangrijkste informatie hierover. Maar het is nog altijd vrij algemene informatie. Om een camerasysteem te kunnen aanschaffen en beheren is veel technische kennis nodig. Alle onderdelen in het camerasysteem moeten ook optimaal op elkaar worden afgesteld: camera's, verbindingen, opslag, software. Het heeft geen enkele zin een camera met 10 megapixel aan te schaffen als het netwerk te weinig bandbreedte heeft en de opslagruimte te beperkt is voor zo'n hoge beeldkwaliteit.

Betekent dit dat elk ziekenhuis zich moet verdiepen in cameratechnologie en alle schakels in de videoketen tot op detailniveau moet doorgronden? Dat kan, maar dat hoeft niet. Er zijn ziekenhuizen die er inderdaad voor kiezen de technische kennis in huis te willen hebben. Zij hebben een technische staf die camerasystemen aanschaft, installeert en beheert. Maar er zijn ook ziekenhuizen waar de technische kennis ontbreekt, of waar de technici andere prioriteiten krijgen. In die gevallen kan een ziekenhuis er ook voor kiezen in zee te gaan met een *system integrator*. Dat is een bedrijf dat in opdracht van het ziekenhuis ervoor zorgt dat een goed werkend camerasysteem wordt aangeschaft en operationeel blijft. Die externe partij onderhandelt namens het ziekenhuis met alle leveranciers en onderaannemers. Hun taak is het om ervoor te zorgen dat het camerasysteem werkt en biedt wat het ziekenhuis nodig heeft. Dit kan in een *service level agreement* worden vastgelegd, inclusief een onderhoudsplan en protocol voor storingsafhandeling.

4. Juridische zaken

Dit hoofdstuk gaat over de juridische aspecten van camera's in ziekenhuizen. Eerst worden de belangrijkste wetten besproken. Dan volgt een overzicht van de belangrijkste juridische uitgangspunten. Speciale aandacht is er voor DPIA's, de rollen van de verschillende instanties in de AVG en informatievoorziening richting betrokkenen. Het hoofdstuk sluit af met de doelen waar camerabeelden voor mogen worden gebruikt: aangifte, vordering, klacht, integriteitsonderzoek en inzageverzoeken.

4.1 De belangrijkste wetten in het kort

Algemene Verordening Gegevensbescherming
De AVG bepaalt hoe persoonsgegevens moeten worden verwerkt. Hierin staat bijvoorbeeld op welke grondslagen gegevens mogen worden verwerkt. Ook de verplichting om een Data Protection Impact Assessment op te stellen volgt uit de AVG.

Arbowet en Burgerlijk Wetboek
Deze twee wetten bevatten artikelen die werkgevers verplichten een veilige werkplek te bieden aan hun personeel: Burgerlijk Wetboek Boek 7, artikel 611 en Arbowet, artikel 3. Dat kan in bepaalde gevallen een grondslag bieden voor de inzet van camera's of bodycams ter preventie van agressie en geweld tegen medewerkers.

Grondwet en EVRM
Deze twee wetten bevatten het recht op bescherming van de persoonlijke levenssfeer. Deze fundamentele rechten mogen alleen worden ingeperkt als daar een wettelijke basis voor is en als de inperking noodzakelijk is voor een rechtmatig doel.

Wet politiegegevens
De AVG geldt niet voor persoonsgegevens die worden gebruikt voor opsporingsdoeleinden: daarvoor geldt de Wet politiegegevens (Wpg). Deze wet geldt dus voor camerabeelden die een ziekenhuis verstrekt aan de politie voor opsporing.

Wetboek van Strafrecht
Dit wetboek verbiedt het heimelijk maken van afbeeldingen. Er zijn uitzonderingen mogelijk, maar alleen als daar een specifieke wettelijke grondslag voor is.

Wetboek van Strafvordering
Dit wetboek bepaalt onder andere onder welke voorwaarden en op welke wijze camerabeelden mogen worden gevorderd door opsporingsambtenaren en anderen.

Wet medezeggenschap cliënten zorginstellingen
Deze wet schrijft voor welke besluiten aan de cliëntenraad moeten worden voorgelegd. Niet elke camera valt onder het adviesrecht, maar het is als zorgaanbieder altijd verstandig actief te communiceren met de cliëntenraad en – in geval van afwijkende opvattingen – met de commissie van vertrouwenslieden.

Wet op de geneeskundige behandelingsovereenkomst
Deze wet regelt de rechten en plichten van de patiënt. Zo staat in deze wet dat patiënten recht hebben op privacy en geheimhouding van medische gegevens.

Wet op de ondernemingsraden
Deze wet bepaalt dat personeelsvolgsystemen pas mogen worden ingevoerd na instemming door de ondernemingsraad. Camera's zijn een mogelijk personeelsvolgsysteem: ze zijn geschikt om de aanwezigheid of het functioneren van medewerkers te beoordelen. Daar worden de meeste camerasystemen niet voor gebruikt, maar dat maakt niet uit. Ook als een camera niet als personeelsvolgsysteem zal worden gebruikt, moet de OR instemmen met de camera's.

4.2 De belangrijkste juridische uitgangspunten

AVG: verwerking gegevens over gezondheid alleen in bepaalde gevallen
In artikel 9 van de AVG is vastgelegd dat persoonsgegevens over iemands gezondheid normaal gesproken niet mogen verwerkt. Maar voor ziekenhuizen is een uitzondering gemaakt: hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening mogen medische gegevens verwerken als dat noodzakelijk is voor iemands behandeling of verzorging. En dat mogen ze ook als het noodzakelijk is voor het beheer van het ziekenhuis zelf. Ziekenhuizen mogen op grond van deze uitzondering dus wel degelijk gegevens over gezondheid verwerken en mogen dat ook met camera's doen. Als tenminste wordt voldaan aan alle andere eisen die de AVG en andere wetten stellen aan camera's.

Grondslag "toestemming" is mogelijk, maar onder voorwaarden
Verwerking van persoonsgegevens moet altijd op een grondslag uit de AVG zijn gebaseerd. Een van de mogelijke grondslagen is toestemming (zie artikel 6, lid 1, onder a van de AVG). Deze toestemming moet worden gegeven door de personen waar gegevens van worden verwerkt en moet gelden voor één of meer specifieke doeleinden. Ook moeten de personen waar het over gaat vrijelijk, specifiek, geïnformeerd en ondubbelzinnig toestemming geven. Toestemming kan niet vrijelijk worden verleend als mensen geen echte vrije keuze hebben of als ze nadelige gevolgen ondervinden als ze hun toestemming weigeren of intrekken. Het is aan te raden de verleende toestemming schriftelijk vast te leggen (zie overweging 32 van de AVG voor meer informatie).

Grondslag "gerechtvaardigd belang" is mogelijk, maar na zorgvuldige afweging
Bij bewakingscamera's is het natuurlijk onmogelijk om iedereen die in beeld kan komen eerst toestemming te vragen om te worden gefilmd. Die camera's worden dan ook niet ingezet op basis van toestemming, maar op de grondslag gerechtvaardigd belang (artikel 6, lid 1 onder f van de AVG). Het ziekenhuis heef een gerechtvaardigd belang om personeel, patiënten, bezoekers, gebouwen en hun eigendommen te bewaken. Ook voor de andere doelen waar camera's voor worden gebruikt kan gerechtvaardigd belang soms de grondslag zijn. Maar het is niet genoeg om een gerechtvaardigd belang te hebben: het ziekenhuis moet het gerechtvaardigde belang afwegen tegen de belangen van de personen die in beeld komen van de camera's. Zij hebben immers ook belang bij de bescherming van hun persoonlijke levenssfeer en medische informatie. Als het belang van het ziekenhuis zwaarder weegt dan het belang van de personen die in beeld komen, mag een camera worden ingezet. Die afweging moet expliciet worden gemaakt en vastgelegd.

Medisch beroepsgeheim en verschoningsrecht
Artsen, verpleegkundigen en veel anderen die in ziekenhuizen werken zijn verplicht alles geheim te houden wat ze tijdens hun werk te weten komen over een patiënt. Dat is nodig omdat iedereen erop moet kunnen vertrouwen dat de informatie die je als patiënt deelt, vertrouwelijk blijft. Het medisch beroepsgeheim bestaat uit de geheimhoudingsplicht en het verschoningsrecht. De geheimhoudingsplicht houdt in dat informatie van patiënten in principe geheim moet worden gehouden. Het verschoningsrecht houdt in dat medisch personeel tegenover politie en justitie bepaalde vragen niet hoeft te beantwoorden (artikel 88 van de Wet BIG). Maar het verschoningsrecht is niet absoluut. Er kunnen situaties zijn waarin het wel degelijk is toegestaan medische informatie te verstrekken. Dat kan bijvoorbeeld als iemand een groot risico vormt voor anderen of in gevallen van kindermishandeling of huiselijk geweld. Er zijn zelfs situaties waarin het verplicht is medische informatie te delen, zoals bij infectieziektes. De afweging of de geheimhoudingsplicht mag worden doorbroken zal in de meeste gevallen in overleg met collega's en een jurist van het ziekenhuis of een externe jurist worden gemaakt. Een goede motivatie om de geheimhoudingsplicht te doorbreken (of juist niet) is cruciaal.

Proportionaliteit en subsidiariteit
Een van de belangrijkste wettelijke eisen is dat elke camera noodzakelijk moet zijn. Het is niet eenvoudig om aan te geven welke camera noodzakelijk is en welke niet. Het vaststellen van de noodzakelijkheid vereist altijd een afweging tussen verschillende belangen. Aan de ene kant hebben medewerkers, patiënten en bezoekers belang bij bescherming van hun persoonlijke levenssfeer. Aan de andere kant kan het ziekenhuis een belang hebben bij bijvoorbeeld beveiliging. En ook patiënten kunnen een belang hebben bij

camera's als die worden ingezet in het kader van patiëntenzorg. Alle belangen moeten uitdrukkelijk tegen elkaar worden afgewogen. Als de camera's een onevenredige schending van het recht op bescherming van de persoonlijke levenssfeer opleveren, zijn ze niet toegestaan. Maar hoe bepaal je dat? Uit de jurisprudentie blijkt dat een camera noodzakelijk is als deze proportioneel en subsidiair is.

Proportioneel

Een camera is proportioneel als de camera gerechtvaardigd wordt door het doel en niet verder gaat dan nodig is voor dat doel. Simpel gezegd: je mag niet met een kanon op een mug schieten. Dus als een ziekenhuis een bewakingscamera wil ophangen op een plek waar nog nooit een incident is gebeurd, is dat niet proportioneel. Maar een camera plaatsen in een fietsenstalling waar daadwerkelijk fietsen zijn gestolen is wel proportioneel. Maar het is dan weer niet proportioneel om in een kleine fietsenstalling honderd camera's op te hangen: dat gaat verder dan nodig voor het doel. Ook is het niet proportioneel om meer plekken in beeld te brengen dan noodzakelijk. Het is dus niet proportioneel om in de wijde omgeving van het ziekenhuis op openbare wegen richting het ziekenhuis camera's met kentekenherkenning te plaatsen als het doel is om fietsendiefstallen uit de stalling tegen te gaan. Niet alleen het aantal camera's en de plaatsing doen ertoe: ook de kijkhoek is van belang. Richt camera's altijd zo precies mogelijk alleen op die plekken die in beeld moeten worden gebracht en film niet meer dan noodzakelijk. De proportionaliteit van een camerasysteem hangt verder ook nog af van de toegang tot de beelden. Camera's zijn meer proportioneel naarmate er minder mensen toegang hebben tot de beelden. Ook de bewaartermijn van de opnames weegt mee: hoe korter de bewaartermijn, hoe proportioneler het camerasysteem. Ook een goeie beveiliging maakt camera's proportioneler. Elke maatregel die de privacy risico's kleiner maakt, maakt de proportionaliteit van de camera groter.

Subsidiair

Van subsidiariteit is sprake als het ingezette middel – dus een camera – het lichtste middel is waarmee het beoogde doel kan worden bereikt. Camera's zijn een relatief zwaar middel omdat ze een inbreuk maken op de privacy van iedereen die in beeld komt. Daarom verdienen lichtere middelen de voorkeur. Dus als een hek of een slot op de deur inbraken of fietsendiefstallen kan voorkomen, is een camera niet subsidiair. Maar als er ondanks dat soort bouwkundige en organisatorische maatregelen toch nog steeds inbraken worden gepleegd en fietsen worden gestolen, kan het soms gerechtvaardigd zijn een camera op te hangen. Camera's zijn vaak de enige manier waarop goed onderbouwd aangifte kan worden gedaan na een incident. Er zijn geen 'lichtere' middelen waarmee datzelfde doel kan worden bereikt. In dat geval is een camera subsidiair. Het is onmogelijk te bewijzen dat er geen enkele lichtere maatregel is; meestal is de onderbouwing van de subsidiariteit gebaseerd op het feit dat de camera's het sluitstuk zijn van een breed pakket aan andere maatregelen.

Het is belangrijk om de afweging van de proportionaliteit en subsidiariteit van de camera's schriftelijk vast te leggen. Dat bewijst immers dat hier goed over is nagedacht. De onderbouwing kan worden opgeschreven in een camerahandboek of -reglement. Maar nog beter is het om een Data Protection Impact Assessment op te stellen voor alle camera's in het ziekenhuis. Daarin wordt beschreven hoe groot het probleem is dat de camera's moeten voorkomen (proportionaliteit) en welke andere, lichtere, maatregelen al zijn getroffen (subsidiariteit). De verwerkingsverantwoordelijke moet in die DPIA vervolgens expliciet de afweging maken tussen het belang bij veiligheid enerzijds en het recht op privacy anderzijds.[1]

1 Dit voorbeeld gaat uit van de grondslag 'gerechtvaardigd belang' (artikel 6.1.f AVG). Als de grondslag 'toestemming' (artikel 6.1.a AVG) is gekozen, is de redenering eenvoudiger. Maar toestemming is vaak geen optie.

4.3 Data Protection Impact Assessment

De AVG (artikel 35) en de Wet politiegegevens (artikel 4c) bevatten de verplichting een Data Protection Impact Assessment op te stellen. In het Nederlands wordt dat een gegevensbeschermingsbeoordeling (GEB) genoemd, maar het is hetzelfde. Deze verplichting geldt alleen voor verwerkingen die een hoog risico opleveren voor de betrokkenen. Cameratoezicht valt al snel in die categorie en daarom is het verstandig een DPIA op te stellen.
In een DPIA moeten een paar onderwerpen worden besproken. De DPIA begint met een beschrijving van de verwerking van persoonsgegevens. Wat gaat u precies doen en op welke manier worden de camerabeelden gemaakt, bekeken, gedeeld, opgeslagen en verwijderd? Daarna moet worden beschreven waarom het ziekenhuis denkt dat inzet van camera's rechtmatig is. In dat hoofdstuk gaat het dus over de grondslag, de noodzakelijkheid, proportionaliteit en subsidiariteit. De verschillende belangen worden tegen elkaar afgewogen. Daarna volgt een hoofdstuk met risico's van de gegevensverwerking en daarna een hoofdstuk met maatregelen om die risico's weg te nemen of te verkleinen.

Een DPIA is uiteindelijk een document met tekst. Maar het proces van het maken van de DPIA is minstens zo belangrijk als het uiteindelijke resultaat. Een goed voorbeeld is "privacy awareness" onder medewerkers: vaak wordt in een DPIA gezegd dat hieraan zal worden gewerkt om zo de gegevensbescherming te bevorderen. Maar dat moet verder gaan dan een afspraak op papier.
De mensen die met het camerasysteem gaan werken moeten worden meegenomen in de discussie zodat ze gaan begrijpen wat de wet zegt en waarom privacy belangrijk is. Daarom is het raadzaam een klein team bij elkaar te roepen voor het maken van de DPIA. Daarin moet in elk geval een privacy officer of privacy functionaris zitten die verstand heeft van de AVG. Daarnaast is het van belang iemand met verstand van informatiebeveiliging en ICT in het team te hebben. Verder moet er natuurlijk iemand in het team zitten die behoefte heeft aan de camera's: die persoon kan aangeven waar de camera's voor nodig zijn. In een tweede cirkel rondom het kernteam kunnen andere deskundigen informatie op afroep aanbieden. Denk aan mensen van inkoop, facilitaire zaken en de ondernemingsraad.

Als de DPIA zo goed als afgerond is, moet de Functionaris voor Gegevensbescherming van het ziekenhuis om advies worden gevraagd. Dat advies kan drie kanten op gaan: negatief, positief of positief met voorwaarden. Het is aan de verwerkingsverantwoordelijke (de directie) om te bepalen of het advies al dan niet wordt overgenomen. Dan kan de DPIA worden vastgesteld en kunnen de risicobeperkende maatregelen worden getroffen. Daarna kan de verwerking starten. Het is raadzaam elke DPIA na een paar jaar een update te geven.

4.4 Verwerkingsverantwoordelijke, verwerker en subverwerker

Er zijn globaal gesproken drie soorten 'rollen' van belang volgens de AVG bij het verwerken van camerabeelden.

Verwerkingsverantwoordelijke
Het ziekenhuis is in de meeste gevallen de "verwerkingsverantwoordelijke". Dat is namelijk de instantie die het doel en de middelen van de camera's vaststelt. De verwerkingsverantwoordelijke moet ervoor zorgen dat alles wat met de camerabeelden gebeurt voldoet aan de AVG. Die verantwoordelijkheid kan nooit aan een ander worden overgedragen of 'doorgeschoven'. Dus als een andere instantie of persoon die niet onder het rechtstreeks gezag van het ziekenhuis staat toegang krijgt tot de camerabeelden, moet het ziekenhuis als verwerkingsverantwoordelijke zorgen dat ook dat verdere gebruik van de camerabeelden aantoonbaar aan de AVG voldoet.

Verwerker
Als het ziekenhuis camerabeelden laat verwerken door een organisatie of persoon die niet onder het rechtstreekse gezag van het ziekenhuis staat, is die ander vaak een "verwerker". Dat is bijvoorbeeld het geval als de camerabeelden naar een particuliere alarmcentrale (PAC) gaan waar beveiligers de beelden bekijken. Die PAC is verwerker van de camerabeelden in opdracht van de verwerkingsverantwoordelijke: het ziekenhuis. De taak van de verwerker wordt bepaald door de verwerkingsverantwoordelijke. Daar ligt dus ook altijd een contract aan ten grondslag: de hoofdovereenkomst. Onder verwijzing

naar de hoofdovereenkomst moeten de verwerkingsverantwoordelijke en de verwerker een verwerkersovereenkomst sluiten. Het doel van die overeenkomst is zorgen dat de verwerker zich houdt aan de AVG en aan de instructies van de verwerkingsverantwoordelijke (zie artikel 28 en 29 van de AVG). In die verwerkersovereenkomst moet staan waar de verwerking over gaat (aard en doel van de verwerking), hoelang de verwerking duurt en over welke persoonsgegevens het gaat. Ook moet daarin worden vastgelegd dat de verwerker de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, dat de medewerkers van de verwerker de gegevens vertrouwelijk behandelen en dat de verwerker actief meehelpt bij het voorkomen van datalekken en het informeren van betrokkenen als zij inzage willen in hun persoonsgegevens. Er zijn online verschillende voorbeelden van verwerkersovereenkomsten te vinden: in de bijlage van deze handreiking staan twee links.

Subverwerker
Een “subverwerker” is een persoon of organisatie die wordt ingehuurd door een verwerker. Bijvoorbeeld een bedrijf dat cloudopslag levert aan een cameraleverancier. De verwerker moet ervoor zorgen dat elke subverwerker zich aan dezelfde afspraken houdt die in de verwerkersovereenkomst staan. Daarom worden in de verwerkersovereenkomst vaak afspraken gemaakt over de manier waarop verwerkers subverwerkers mogen inschakelen. Er zijn hier globaal twee opties:

- De eerste optie is om van elke verwerker te eisen dat deze de verwerkingsverantwoordelijke eerst informeert voordat een subverwerker wordt ingeschakeld. Deze optie is gekozen in de model verwerkersovereenkomst van de Brancheorganisaties in de Zorg (artikel 7.1). In die verwerkersovereenkomst staat dat de verwerker het plan om een nieuwe subverwerker in te schakelen drie maanden van tevoren moet mededelen aan de verwerkingsverantwoordelijke. Op die manier houdt de verwerkingsverantwoordelijke de regie over de inzet van subverwerkers.
- De tweede optie is om de verwerker het recht te geven een subverwerker in te schakelen, als de verwerker die subverwerker maar aan dezelfde afspraken houdt. Die optie is gekozen in de model verwerkersovereenkomst van de Vereniging Nederlandse Gemeenten (artikel 4.5). In dit geval moet de verwerkingsverantwoordelijke er dus op rekenen dat de verwerker deze afspraak netjes zal nakomen.

Intern beheer
Als een afdeling, organisatie of individu onder rechtstreeks gezag van de verwerkingsverantwoordelijke (dus het ziekenhuis) camerabeelden verwerkt, valt dat onder intern beheer. Het ziekenhuis kan bijvoorbeeld een beveiliger van een extern bedrijf inhuren om camerabeelden te bekijken. Omdat die beveiliger onder rechtstreeks gezag staat van het ziekenhuis, is sprake van intern beheer – ook als de beveiliger werknemer is van een ander bedrijf. Dat geldt ook voor de situatie dat een medewerker van een verpleegkundige afdeling camerabeelden bekijkt die door de afdeling beveiliging zijn gemaakt. Beide afdelingen staan onder rechtstreeks gezag van dezelfde verwerkingsverantwoordelijke: het ziekenhuis. Ook in dat voorbeeld is dus geen sprake van een verwerker, maar van intern beheer. Dan is dus ook geen verwerkersovereenkomst nodig.

4.5 Informeren van betrokkenen

Het is van groot belang iedereen te informeren over de aanwezige camera’s. Dat is een wettelijke plicht, maar het heeft nog een groot voordeel: het kan het preventieve effect van camera’s vergroten en het kan zorgen voor een groter veiligheidsgevoel. Daarnaast is communicatie over camera’s belangrijk omdat het eventuele zorgen van medewerkers, patiënten en bezoekers kan wegnemen.

Het is van groot belang hier vooraf goed over na te denken. Een voorbeeld hoe het *niet* moet haalde het landelijke nieuws. Een zorginstelling had zonder overleg met de bewoners camera’s in verpleeghuiskamers geïnstalleerd. Vragen van bewoners en hun familie kon de zorginstelling niet beantwoorden, maar het verhaal was dat de camera’s niet aan stonden. Maar op de camera’s waren lampjes te zien die afwisselend rood en groen kleurden. De bewoners vonden dat verdacht en bleven daarom vragen stellen. Na enige tijd kwamen er technici van een cameraleverancier in alle verpleeghuiskamers om de camera’s uit te schakelen. Blijkbaar stonden de camera’s dus toch aan. Dat

leverde uiteraard weer nieuwe onrust en onvrede op bij de bewoners en hun familie. Ook het personeel was volgens het krantenbericht ‘in rep en roer’. Dit soort onduidelijkheid is natuurlijk zeer onwenselijk als ergens camera’s worden geplaatst. Daarom is een goed voorbereide informatievoorziening zo belangrijk.

Richtlijnen over informatieborden of -stickers

Er is geen wet die bepaalt wat er op een bordje of sticker over cameratoezicht moet staan.[2] Er is wel een richtlijn van de European Data Protection Board (EDPB) – de koepelorganisatie van alle nationale autoriteiten die toezicht houden op naleving van de AVG.[3] Volgens die richtlijn moet informatie in twee lagen worden aangeboden: een eerste fysieke laag (bordje of sticker) en een tweede laag (website of een informatiefolder bij de receptie).

1. Eerste laag
- Er moeten informatiebordjes of -stickers zijn met begrijpelijke en goed leesbare informatie over de beoogde verwerking van de camerabeelden;
- Elke betrokkene moet deze informatie kunnen lezen voordat hij of zij in beeld van de camera komt;
- Het moet duidelijk zijn wie de verwerkingsverantwoordelijke is, het doel van de camera’s, de rechten van de betrokkene en bij voorkeur ook de grondslag voor de verwerking en contactgegevens van de verwerkingsverantwoordelijke;
- Tevens moet duidelijk zijn waar mensen meer informatie kunnen vinden.

2. Tweede laag
- In een folder bij de balie of een pagina op een website moet alle informatie staan die verplicht is gesteld in art. 13 van de AVG;
- Het gaat dan bijvoorbeeld om de bewaartermijn, het recht op inzage, het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens en of er automatische besluitvorming plaatsvindt op basis van de beelden.

De meeste ziekenhuizen kiezen ervoor op hun website een algemene privacyverklaring op te nemen met daaronder een specifieke privacyverklaring voor bijzondere of gevoelige verwerkingen van persoonsgegevens. Een specifieke privacyverklaring voor camera’s is dan een goed idee. Vaak wordt de inzet van camera’s ook opgenomen in de huisregels van het ziekenhuis.

Veel ziekenhuizen kondigen hun camera’s momenteel wel aan met bordjes of stickers. Maar in veel ziekenhuizen staat daarop nog niet alle informatie die daar volgens de AVG, AP en EDPB op zou moeten staan. Ook de websites van veel ziekenhuizen bieden nog niet de informatie waar mensen recht op hebben. De Europese richtlijn van de EDPB waar hierboven naar werd verwezen geeft aan welke informatie moet worden aangeboden.

Heimelijke camera’s

Overigens is het ook mogelijk – in bijzondere gevallen en alleen als de ondernemingsraad instemt – heimelijke camera’s te plaatsen. Dat kan bijvoorbeeld noodzakelijk zijn om te kunnen bewijzen dat een medewerker die wordt verdacht van strafbare feiten, zoals diefstal, inderdaad spullen steelt. Omdat het heimelijk cameratoezicht is, is de inbreuk op de privacy zeer groot. Daar zijn dan ook stevige waarborgen voor nodig en het mag alleen worden ingezet in specifieke gevallen en alleen in opdracht van de directie. Advies van een juridisch specialist is een goed idee als de inzet van heimelijk cameratoezicht wordt overwogen.

2 Voor camerabewaking in België is het pictogram voor camerabewaking wel wettelijk vastgesteld. Zie: https://www.ejustice.just.fgov.be/mopdf/2008/02/21_1.pdf#Page11.

3 Zie: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf. Een voorbeeld pictogram staat op pagina 13 van deze richtlijn.

4.6 Gebruik van opnames

Verstrekking van beelden aan de politie na een vordering
Opsporingsambtenaren mogen bij verdenking van bepaalde misdrijven opnames van bewakingscamera's vorderen op grond van artikel 126nda van het Wetboek van Strafvordering. Dat wetsartikel is beperkt tot beelden gemaakt met camera's voor de beveiliging van goederen, gebouwen of personen. Daarnaast zijn er functionarissen met bredere bevoegdheden: de officier van justitie mag gegevens vorderen op grond van artikel 126nd van het Wetboek van Strafvordering. In sommige situaties heeft de officier van justitie daar een machtiging van een rechter-commissaris voor nodig (artikel 126nf Wetboek van Strafvordering).

Het ziekenhuis moet na het ontvangen van een vordering de afweging maken of de opnames verstrekt zullen worden. Het ziekenhuis moet allereerst vaststellen of de ontvangen vordering passend is voor de gevorderde gegevens. Ook moeten de vordering en de identiteit van de vorderende ambtenaar worden gecontroleerd. Het ziekenhuis hoeft niet te beoordelen of de opnames bruikbaar zijn voor het opsporingsonderzoek. Het ziekenhuis moet wel bepalen of het medisch beroepsgeheim van toepassing is en of verstrekking kan leiden tot ernstige schade aan de vertrouwensrelatie met de patiënt. Kortom: het kan gebeuren dat een ziekenhuis tot het oordeel komt dat camerabeelden niet met de politie mogen worden gedeeld. Het ziekenhuis beroept zich dan op het verschoningsrecht en weigert de informatie te geven. In een enkel geval worden beelden 'onder protest' van het ziekenhuis verstrekt. Juridisch advies is in alle gevallen raadzaam.

Als het gaat om beelden van een bewakingscamera aan de buitenkant van het ziekenhuis waarmee een inbreker of autodief is gefilmd, zal er meestal geen bezwaar zijn de beelden te verstrekken. Maar camerabeelden die in het ziekenhuis zijn gemaakt kunnen medische informatie bevatten. En bij camera's die in het kader van medisch onderzoek of behandeling zijn gemaakt geldt dat zeker: die camerabeelden maken onderdeel uit van het medisch dossier. Die beelden moeten in beslag worden genomen op grond van artikel 105 Sv. Maar ook dan moet het ziekenhuis beslissen of het medisch beroepsgeheim wordt doorbroken.

Het is mogelijk dat er aanvullende afspraken zijn gemaakt tussen ziekenhuizen, politie en Openbaar Ministerie. In de regio Amsterdam en Noord Holland is bijvoorbeeld in een SIGRA convenant en bijbehorende handreiking afgesproken dat ziekenhuizen en zorginstellingen geen camerabeelden verstrekken na een vordering door een opsporingsambtenaar (art. 126nda Sv). Zij verstrekken alleen als er minimaal een vordering is afgegeven door een officier van justitie (art. 126nd Sv) of rechter-commissaris (126nf Sv). Ook in de regio Rotterdam is in het SRZ-convenant met handreiking een afspraak hierover gemaakt. Het Openbaar Ministerie heeft daar de keuze gemaakt alleen gebruik te maken van artikel 126nd Sv. Overigens kan het ziekenhuis (de 'verschoningsgerechtigde') overigens nog altijd een beroep doen op het beroepsgeheim of het verschoningsrecht. De rechter-commissaris moet beslissen over dat beroep (art. 98 Sv).

Verstrekking van beelden aan politie op initiatief van het ziekenhuis
Het is toegestaan om als ziekenhuis zelf het initiatief te nemen camerabeelden aan de politie te verstrekken. Dat kan bijvoorbeeld na een inbraak, diefstal of een vernieling. Of als een medewerker van het ziekenhuis slachtoffer is geworden van bedreiging, belediging of mishandeling. In die gevallen kan het ziekenhuis een kopie van beeldopnames aan de politie verstrekken om de aangifte te onderbouwen. Dat kan zonder vordering, maar alleen als het ziekenhuis de beelden *vrijwillig* en *ongevraagd* aan de politie verstrekt. Vooral de voorwaarde dat de beelden ongevraagd moeten zijn verstrekt wordt wel eens vergeten. Als de politie het ziekenhuis vraagt camerabeelden vrijwillig af te geven is geen sprake meer van ongevraagde afgifte. In dat soort gevallen is vordering wenselijk: "vragen = vorderen".[4]

4 Zie: Arrest van de Hoge Raad 21 december 2010, ECLI:NL:HR:2010:BL7688, NJ 2012/24, m.nt. Borgers. Zie ook: HR 27 november 2012, ECLI:NL:HR:2012:BY0215, NJ 2012/693.

Sommige ziekenhuizen hanteren zelf een strenger beleid en verstrekken camerabeelden uitsluitend na een vordering aan de politie. Dat is geen wettelijke eis, maar het is wel een manier om eventuele discussies in de rechtbank te voorkomen.[5] Er zijn voor ziekenhuizen overigens goede redenen om terughoudend te zijn in het verstrekken van camerabeelden aan de politie. Camerabeelden uit een ziekenhuis kunnen immers medische informatie bevatten en zoals gezegd is daarop het medisch beroepsgeheim van toepassing. Maar het medisch beroepsgeheim mag in specifieke gevallen worden doorbroken. Het ziekenhuis zal expliciet moeten afwegen wat zwaarder weegt: het belang van het ziekenhuis bij de beveiliging van goederen, gebouwen en personen of het belang van personen bij de bescherming van hun privacy en het waarborgen van het medisch beroepsgeheim. Het is raadzaam hierover met een intern juridisch adviseur te overleggen voordat camerabeelden worden verstrekt aan de politie.

Blurren van beelden hoeft niet tot bewijsuitsluiting te leiden

Omwille van privacybescherming kiezen sommige ziekenhuizen ervoor omstanders die niets met het incident te maken hebben onherkenbaar te maken in de beelden voordat ze aan de politie worden verstrekt. Dit wordt vaak 'blurren' genoemd en het is een ingebouwde optie in bepaalde videomanagementsystemen. Volgens sommige medewerkers van ziekenhuizen en de politie leiden dergelijke bewerkingen er echter toe dat de authenticiteit van het beeldmateriaal ter discussie kan worden gesteld. Dat zou er vervolgens weer toe kunnen leiden dat het bewijsmateriaal wordt uitgesloten door de rechter. Maar dat *hoeft* niet te gebeuren. Het is wel degelijk mogelijk bewerkte camerabeelden te gebruiken als bewijs als het ziekenhuis een verklaring meegeeft welke bewerking is uitgevoerd (blurren van personen die niets met het incident te maken hebben) en waarom voor die bewerking is gekozen (bescherming van privacy en medisch beroepsgeheim). Dan kan de rechter kennis nemen van de beelden en deze gebruiken als bewijs.

5 Zie: Parket bij de Hoge Raad ECLI:NL:PHR:2015:2260.

Klachtafhandeling

Het is juridisch gezien mogelijk camerabeelden te gebruiken voor het behandelen van klachten. Dit moet dan wel zijn vastgelegd in het klachtenreglement van het ziekenhuis. Ook moet duidelijk zijn wie precies bevoegd is om de camerabeelden op te vragen. Bijzonder aan klachtenbehandeling is dat er in vrijwel alle gevallen eerst een informele fase wordt doorlopen. Als een patiënt bijvoorbeeld een klacht heeft over een arts of verpleegkundige is het meestal zo dat eerst een persoonlijk gesprek wordt gevoerd. Daar zal vaak de leidinggevende bij aanwezig zijn. Als dat gesprek niet tot tevredenheid bij de klager leidt, kan een formele fase worden gestart. Dan gaat de klachtenfunctionaris aan het werk, meestal eerst in de vorm van een bemiddeling, maar daarna mogelijk ook via een formeel onderzoek naar feiten en omstandigheden. Dat formele onderzoek is dan het moment waarop behoefte aan camerabeelden zou kunnen ontstaan. Maar tegen die tijd zijn er meestal een paar weken of maanden verstreken en zijn de opgenomen camerabeelden meestal al automatisch verwijderd. Om dit te voorkomen zullen er dus afspraken moeten worden gemaakt in een camerabeleid over het veilig stellen van camerabeelden 'voor het geval dat' ze nodig zijn voor klachtafhandeling. Dit moet in een camerabeleid worden vastgelegd.

Integriteitsonderzoek naar een medewerker

Als een medewerker wordt verdacht van een integriteitsschending kan een integriteitsonderzoek worden uitgevoerd. Die onderzoeken kunnen gaan over alle feiten die in het personeelsreglement worden genoemd als integriteitsschending. Denk aan diefstal, fraude, corruptie, discriminatie, intimidatie, belangenverstrengeling, schending geheimhoudingsplicht en dergelijke. Meldingen van integriteitsschendingen komen meestal binnen bij het Bureau Integriteit van het ziekenhuis, maar kunnen ook bij een leidinggevende binnenkomen. Meldingen van integriteitsschendingen worden meestal eerst besproken met een interne adviseur integriteit om te zien welke vervolgstappen passend zijn. De directie kan besluiten opdracht te geven tot het uitvoeren van een integriteitsonderzoek. Dat onderzoek bestaat meestal uit een oriënterende fase en een feitenonderzoek. In de oriënterende fase worden geen onderzoeksmethoden ingezet die een grote inbreuk maken op de privacy. Als daarna wordt besloten ook een feitenonderzoek in te stellen, wordt dat vaak

uitgevoerd door een interne of externe onderzoeker die ook de bevoegdheid heeft om opnames gemaakt met camera's te bekijken. De onderzoeker kan de betreffende opname laten veiligstellen en is bevoegd een kopie op te vragen voor het onderzoek. Maar net als bij klachtafhandeling geldt hiervoor dat de bewaartermijn dan vaak al lang is verstreken waardoor de beelden niet meer beschikbaar zijn. Dus als het de bedoeling is beelden hiervoor alvast veilig te stellen voor een eventueel later moment, zal daar een procedure voor moeten worden afgesproken en vastgelegd in het camerabeleid. Uiteraard hoort daar ook een procedure bij voor het weer verwijderen van veilig gestelde opnames die achteraf toch niet nodig bleken te zijn.

Inzageverzoek van een betrokkene
Betrokkenen (dat zijn alle personen die door een camera worden gefilmd) hebben recht op inzage in hun eigen persoonsgegevens. Betrokkenen kunnen een inzageverzoek indienen bij het ziekenhuis. Die verzoeken worden meestal behandeld door een privacy officer of een interne jurist. Als wordt besloten inzage te geven, wordt de relevante opname veilig gesteld en getoond aan de betrokkene. Het verdient aanbeveling opnames te laten bekijken in een afgeschermde ruimte in het ziekenhuis zelf en geen kopie te verstrekken. Het is van belang te benadrukken dat het recht op inzage niet bedoeld is om mensen in staat te stellen te beoordelen of ze een klacht willen indienen of aangifte willen doen. Het recht op inzage gaat alleen over de vraag of er persoonsgegevens van de betrokkene worden verwerkt. De betrokkene kan ook uitsluitend inzage in de eigen persoonsgegevens krijgen: alle informatie over andere patiënten, bezoekers en personeel (video, maar ook audio) moet dus onherkenbaar worden gemaakt.

5. Vraag & Antwoord

Helaas is het vaak niet mogelijk een eenvoudig antwoord te geven op juridische vragen over camera's in ziekenhuizen. Het wordt al snel ingewikkeld omdat de juridische afwegingen afhangen van de specifieke situatie, de omstandigheden en de gebruikte techniek. Vaak moeten verschillende belangen tegen elkaar worden afgewogen. Privacybescherming is een groot goed, maar beveiliging van het ziekenhuis en de medewerkers is ook belangrijk. Dus in het ene geval mag een camera wel worden gebruikt en in het andere geval niet. Hoe die afweging in een specifiek geval uitpakt, kan niet in algemene vuistregels worden samengevat. In dit hoofdstuk worden dan ook geen simpele antwoorden gegeven, maar worden enkele veelvoorkomende juridische vragen besproken, inclusief de nuanceringen.

Hoe lang mag je camerabeelden bewaren?
Veel camerabeelden worden 28 dagen bewaard. Die termijn wordt door velen als een wettelijke standaard beschouwd. Maar dat is niet juist: er is geen wettelijke bewaartermijn voor camerabeelden. De wetgeving bepaalt slechts dat beelden niet langer mogen worden bewaard dan noodzakelijk voor het doel. Dat betekent dat de maximale bewaartermijn heel verschillend kan zijn per camerasysteem. Als een camera nodig is om te zien of de slagboom omhoog moet om auto's toe te laten, is het voldoende de beelden hooguit een paar seconden op te slaan. Als het daarentegen nodig is om een opgenomen gesprek met een patiënt te bewaren in het kader van een gerechtelijke procedure, kan die specifieke opname enkele jaren bewaard moeten worden. De bewaartermijn hangt dus af van het doel. Het enige juridische criterium is dat beelden niet langer mogen worden bewaard dan noodzakelijk voor het doel.

Wat houdt de eis van doelbinding in?
Het moet voor betrokkenen vooraf duidelijk en voorspelbaar zijn wat er met hun persoonsgegevens kan gebeuren. Daarom is doelbinding een belangrijke voorwaarde voor alle camerasystemen. Gebruik van camerabeelden moet beperkt blijven tot die doelen waar de camera oorspronkelijk voor is geïnstalleerd. Het doel van een camera moet welbepaald, uitdrukkelijk

omschreven en gerechtvaardigd zijn (dit volgt uit artikel 5, lid 1 van de AVG). Het doel moet ook worden bepaald vóórdat de camera in gebruik wordt genomen: dat mag niet tijdens het verzamelen of verwerken van de gegevens worden gewijzigd. Het doel mag ook niet worden opgerekt: de verwerking van de camerabeelden moet te allen tijde verenigbaar zijn met het oorspronkelijke doel.

Soms is het heel eenvoudig te bepalen waar de grens ligt. Het is vrij logisch dat het niet is toegestaan beelden van een camera die voor bewaking is opgehangen te gebruiken in een online promotiefilmpje op de website van het ziekenhuis. Maar soms is het moeilijker te bepalen: mag je camerabeelden van de ontvangsthal analyseren om de wachttijden te verkorten en de dienstverlening te verbeteren? Mag je bewakingscamera's ook gebruiken voor het tellen van het aantal personen dat passeert? Onder bepaalde voorwaarden mogen camera's voor meerdere doelen worden gebruikt. Camerabeelden van een bewakingscamera die vooral preventief is bedoeld, mogen door de politie worden gebruikt voor opsporing na bijvoorbeeld een inbraak of diefstal. Opsporing wordt daarom soms "bijvangst" van dit soort bewakingscamera's genoemd. Het niet het hoofddoel, maar het kan er wel voor worden gebruikt. Dat geldt trouwens ook voor andere camera's, zoals smartphones. Die zijn niet bedoeld voor opsporing, maar als iemand iets filmt dat van belang is voor de politie, mogen die beelden wel degelijk aan de politie worden verstrekt. Die beelden mogen daarna ook door de politie worden gebruikt voor opsporing, ondanks het feit dat de camera oorspronkelijk niet was bedoeld voor opsporing. Bij het overdragen van camerabeelden aan de politie is het belangrijkste dat dit rechtmatig gebeurt. Dat kan op twee manieren: vrijwillige en ongevraagde verstrekking of na een vordering. Het verstrekken van camerabeelden aan de politie is behandeld in het vorige hoofdstuk.

Wat is meervoudig cameragebruik en mag het?
Soms is het handig om een camera die voor doel A is opgehangen ook te gaan gebruiken voor doel B. In die gevallen spreken we van meervoudig cameragebruik. Dat is echter niet altijd toegestaan. Want het gaat tegen de eis van doelbinding in. Maar onder bepaalde voorwaarden is meervoudig gebruik van een camera wel mogelijk. Dat is – kort gezegd – het geval als het ziekenhuis ook een aparte camera zou mogen ophangen voor doel B. In dat geval mag de reeds aanwezige camera voor doel A ook voor doel B worden gebruikt. Dat moet dan overigens wel worden geregeld in alle juridische documentatie en ook de informatiebeveiliging moet goed worden doordacht. Over meervoudig cameragebruik is veel informatie beschikbaar op de website van de *Adviesfunctie verantwoord datagebruik*.[6]

Wanneer is heimelijk cameratoezicht toegestaan?
Heimelijk cameratoezicht is in verreweg de meeste gevallen verboden. Dit staat in het Wetboek van Strafrecht. Er zijn twee aparte verbodsbepalingen: voor openbare plaatsen en voor niet-openbare plaatsen. De reden dat dit verschil wordt gemaakt is dat mensen op openbaar toegankelijke plekken een andere verwachting hebben van privacy: iedereen weet dat je op straat kan worden gefilmd. Maar in een woning, spreekkamer of operatiekamer verwacht je niet dat je wordt gefilmd. Daarom gelden daar strengere regels en kan een langere gevangenisstraf of boete worden opgelegd aan overtreders.

Niet-openbare plaatsen ("binnen")
Artikel 139f verbiedt het wederrechtelijk maken van afbeeldingen van personen in woningen en andere niet voor het publiek toegankelijke plaatsen met een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt.

Openbare plaatsen ("buiten")
Artikel 441b zegt hetzelfde, maar gaat over plaatsen die voor het publiek toegankelijk zijn, zoals buiten op straat. Dus ook op openbare plaatsen is het in principe verboden mensen heimelijk te filmen.

6 De landsadvocaat Pels Rijcken en Verdonck, Klooster & Associates werken samen in de Adviesfunctie verantwoord datagebruik die is opgericht in het kader van de landelijke Interbestuurlijke Datastrategie. Zie de links aan het eind van deze handreiking.

Het is van belang op te merken dat het Wetboek van Strafrecht niet vereist dat mensen door middel van informatieborden of -stickers worden geïnformeerd. De enige eis uit het Wetboek van Strafrecht is dat de aanwezigheid van de camera op duidelijke wijze kenbaar moet zijn. Dus als de camera zelf duidelijk zichtbaar is, is al geen sprake meer van heimelijk filmen.[7] Ander belangrijk detail in beide wetsartikelen is het woord 'wederrechtelijk'. Het is alleen verboden mensen heimelijk te filmen als dat *wederrechtelijk* gebeurt. Dat betekent dat het wel degelijk is toegestaan om heimelijk te filmen als daar een wettelijke basis voor is. Zo'n basis is bijvoorbeeld te vinden in het Wetboek van Strafvordering. Daarin staat welke functionarissen onder welke voorwaarden heimelijk afbeeldingen mogen vervaardigen. Het is in bepaalde gevallen ook toegestaan voor ziekenhuizen om heimelijke camera's in te zetten. Belangrijke voorwaarde is dat het onmogelijk moet zijn het doel te bereiken met een zichtbare camera. Dat kan in een ziekenhuis bijvoorbeeld het geval zijn als een werknemer wordt verdacht van diefstal en er bewijsmateriaal moet worden verzameld. Dan kan het in bepaalde gevallen rechtmatig zijn een heimelijke camera te installeren. Maar alleen in bijzondere gevallen en alleen met zorgvuldige waarborgen.

Welke functionarissen moeten worden betrokken bij camerabeleid?
Voor een goed camerabeleid is input nodig vanuit diverse disciplines. Betrek daarom de volgende afdelingen en/of functionarissen:

- Juridische Zaken
- Privacy Officer
- Functionaris voor Gegevensbescherming
- Ethische commissie
- Information Security Officer
- ICT
- Facilities
- Ondernemingsraad
- Cliëntenraad

7 Overigens is het op grond van de AVG wel degelijk verplicht mensen te informeren over aanwezige camera's.

Wat is de rol van de ondernemingsraad?
Elk ziekenhuis is verplicht de ondernemingsraad instemming te vragen voordat er een systeem wordt ingevoerd dat gericht is op (of geschikt is voor) waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen (zie artikel 27 WOR). Voor het gemak worden dergelijke systemen personeelsvolgsystemen genoemd; die term staat niet in de wet, maar wordt wel vaak gebruikt. Camera's zijn meestal niet bedoeld om de aanwezigheid, gedrag of prestaties van werknemers te controleren, maar ze zijn er wel voor geschikt. En dus mogen camera's alleen worden opgehangen na instemming door de OR.

Het ziekenhuis moet eerst het besluit voorbereiden om camera's in te voeren en beschrijven welke spelregels daarvoor zullen gaan gelden. Daarna wordt instemming gevraagd aan de ondernemingsraad. Dat moet opnieuw gebeuren als de camera's worden verwijderd of als het systeem wordt gewijzigd.
Een belangrijke vraag is altijd of er ook heimelijke camera's mogen worden opgehangen en of beelden ook mogen worden gebruikt voor een integriteitsonderzoek naar een medewerker. Vaak stelt de ondernemingsraad als eis dat ze moeten worden geïnformeerd over elke concrete inzet van heimelijke camera's of gebruik van camera's voor integriteitsonderzoeken. Overigens moeten alle werknemers ook worden geïnformeerd over de mogelijkheid dat ze in beeld komen van (al dan niet heimelijke) camera's en dat ze aan een integriteitsonderzoek kunnen worden onderworpen. Ook het feit dat camerabeelden kunnen worden gebruikt om klachten mee te behandelen, moet worden gemeld aan het personeel. Vaak wordt dat geregeld door hierover een tekst op te nemen in het Personeelsreglement.

Waarom moet je patiënten en bezoekers informeren over camera's?
Heimelijk cameratoezicht is in vrijwel alle gevallen verboden. In alle andere gevallen moeten de patiënten en bezoekers (en medewerkers) dus worden geïnformeerd over de camera's. Dat is een eis die volgt uit de AVG, maar ook uit het verbod in het Wetboek van Strafrecht om mensen heimelijk te filmen. Dat is op zich natuurlijk al meer dan voldoende reden om mensen te informeren. Maar het is ook een goed idee omdat informatie over camera's het preventieve effect en het veiligheidsgevoel kan vergroten. Camera's zelf moeten goed zichtbaar zijn, er moeten informatieborden of -stickers worden opgehangen en

er moet meer informatie te vinden zijn in een folder of op de website van het ziekenhuis. Het is ook raadzaam in de huisregels die worden opgehangen te vermelden dat er cameratoezicht is.

Zijn dummy-camera's een goed alternatief voor echte camera's?
Er zijn camera's te koop die er echt uitzien, maar niet echt zijn. Het is ook mogelijk een echte camera op te hangen, maar deze niet 'aan' te zetten. Dit worden vaak dummy-camera's genoemd. Het idee is dat mensen zich ook door een dummy-camera beter aan de regels zullen houden, zonder dat je aan de AVG hoeft te voldoen zoals bij een echte camera.

In bepaalde gevallen kan een dummy een goed alternatief zijn, maar niet altijd. Van belang is rekening te houden met het feit dat ook dummy-camera's effect hebben op het gedrag van mensen – en dat kan ook een onwenselijk effect zijn. Ook een dummy camera kan er immers toe leiden dat mensen niet naar het ziekenhuis willen komen of bepaalde informatie niet willen delen. Daardoor komt de toegankelijkheid en de kwaliteit van de zorg in gevaar. Een ander risico is dat geen beelden beschikbaar zijn van ernstige incidenten. Het ziekenhuis zal dan moeten toegeven dat een camera niet echt was, maar een dummy. Dat levert bestuurlijke risico's op waar de directie zich vooraf goed bewust van moet zijn. De ethische discussie over de vraag wat wenselijk is ("Wat voor ziekenhuis willen wij zijn?"), is bij dummy-camera's net zo belangrijk als bij echte camera's.

Maakt het uit als beelden niet worden opgenomen, maar alleen live bekeken?
Ja en nee. Hoe meer er met camerabeelden wordt gedaan, hoe groter de risico's. Als een camera live wordt bekeken en als de beelden worden opgenomen, zijn de privacy risico's groter dan als beelden alleen live worden bekeken. Maar ook als een camera alleen maar live wordt bekeken en niet opneemt, zijn er risico's voor de privacy. In juridische zin is het niet zo dat een camera die alleen maar live wordt bekeken als een soort 'uitzondering' kan worden gezien waardoor de privacywetgeving niet zou gelden. Ook het live meekijken met een camera is volgens de AVG een verwerking van persoonsgegevens. Dus ook voor een camera die niet opneemt moet al het juridische "huiswerk" worden gedaan.

Mogen patiënten en bezoekers zelf filmen in een ziekenhuis?
De AVG geldt niet als iemand een foto of filmpje maakt "in het kader van een louter persoonlijke of huishoudelijke activiteit die als zodanig geen enkel verband houdt met een beroeps- of handelsactiviteit". Het maken van een foto-, video- of audio-opname die alleen voor persoonlijk gebruik bedoeld is, is dus geen verwerking van persoonsgegevens die aan de AVG moet voldoen. Dat mag dus ook in een ziekenhuis.[8] In de AVG zijn ook het voeren van correspondentie en sociaal netwerken en online-activiteiten in de context van louter persoonlijke of huishoudelijke activiteit vrijgesteld. Een belangrijke voorwaarde is dat de informatie niet breed mag worden verspreid. Het is dus niet toegestaan om een opname op internet te publiceren waardoor de opname voor een grote groep mensen toegankelijk wordt. Dat valt niet meer onder persoonlijke of huishoudelijke activiteiten. Waar de grens precies ligt tussen delen met een kleine groep en delen met een grote groep mensen is niet hard te trekken, zo blijkt uit de jurisprudentie.

Mag een patiënt een gesprek met een arts of verpleger opnemen?
Veel patiënten zijn gespannen of emotioneel tijdens gesprekken met artsen of verplegers. Daardoor kunnen ze soms niet alle informatie onthouden. Dan is het prettig om een gesprek later te kunnen terugluisteren en te kunnen delen met bijvoorbeeld een familielid of een andere zorgverlener. Daardoor kan het aantal vervolgvragen en -consulten worden verminderd. Ook kan de zorg erdoor worden verbeterd en tot meer gedeelde besluitvorming leiden. Het is niet strafbaar als een patiënt een gesprek met een arts of verpleger opneemt. Dat geldt zelfs voor heimelijk gemaakte geluidsopnames. Het is een kwestie van fatsoen dat patiënten hun arts vooraf vertellen dat ze graag een opname willen maken, maar het is niet verplicht. Het is wel verboden om heimelijk een filmpje te maken, want voor het heimelijk maken van afbeeldingen gelden strengere regels dan voor heimelijke geluidsopnames.[9]

8 Behalve als in de huisregels is opgenomen dat dit niet is toegestaan.

9 Artikel 139f Wetboek van Strafrecht.

Het is ook verboden een opname zonder toestemming te verspreiden buiten de privésfeer: dat geldt voor beeldopnames, maar ook voor geluidsopnames. Aangezien het voor de zorg goed kan zijn om patiënten opnames te laten maken, is het verstandig de 'spelregels' te bespreken en mensen actief uit te nodigen het gesprek op te nemen.

Mag een arts een gesprek met een patiënt opnemen?
Patiënten mogen altijd gesprekken met zorgprofessionals opnemen: andersom geldt dat echter niet. Zorgprofessionals die een opname willen maken moeten vooraf toestemming vragen aan de patiënt. De patiënt moet te horen krijgen wat het doel van de opname is (bijvoorbeeld voor de behandeling van de patiënt of onderwijs) en de bewaartermijn. Het is niet toegestaan de opname later voor een ander doel te gebruiken of langer te bewaren dan noodzakelijk voor het afgesproken doel. Als een opname aan het medisch dossier moet worden toegevoegd geldt voor die opname de wettelijke bewaartermijn voor medische dossiers. Een camera-opname waar een patiënt is te horen of te zien valt onder het medisch beroepsgeheim. Dus zonder toestemming van de patiënt mogen anderen de opname niet zien of horen.

Moet ik een verwerkersovereenkomst sluiten met de leverancier van de camera's?
Het ziekenhuis is de verwerkingsverantwoordelijke: het ziekenhuis bepaalt namelijk het doel (meestal beveiliging) en de middelen (camera's) van de verwerking. Als een extern bedrijf wordt ingehuurd om het camerasysteem te realiseren, te beheren of te gebruiken, is dat vaak een verwerker. Dat geldt ook als de beelden elders worden opgeslagen, zoals bij een cloud-opslag. Als een afdeling of medewerker van het ziekenhuis de gegevens gebruikt, is dat geen verwerker: dat valt onder intern beheer. Maar als het gaat om een bedrijf dat niet aan het rechtstreekse gezag van het ziekenhuis is onderworpen, dan is dat een verwerker in de zin van de AVG. De verwerker heeft geen zeggenschap over de persoonsgegevens: zij handelen onder de verantwoordelijkheid van en volgens de instructies van de verwerkingsverantwoordelijke.

Als een verwerker daarna zelfstandig beslissingen neemt over de doelen van de verdere verwerking en de middelen, dan is die verwerker de verwerkingsverantwoordelijke voor die nieuwe verwerking. Dat zou bijvoorbeeld gebeuren als een leverancier van een camerasysteem in een ziekenhuis daarnaast afspraken maakt met de politie om de camerabeelden door te sturen. Of als een aanbieder van cloudopslag de camerabeelden wil gaan gebruiken voor data-analyse en het trainen van algoritmes. Omdat het ziekenhuis daar geen opdracht voor heeft gegeven aan de verwerker, is de verwerker zelf de verwerkingsverantwoordelijke voor het nieuwe doel. Het ziekenhuis wil natuurlijk niet dat camerabeelden door de verwerker voor dat soort andere doelen worden gebruikt. Daarom wordt een verwerkersovereenkomst gesloten. Daarin staat waar de verwerking over gaat en welke verplichtingen gelden voor de verwerker. Er zijn online verschillende voorbeelden van verwerkersovereenkomsten te vinden: er staan twee links in de bijlage van deze handreiking.

Cameraplanner – een korte routekaart

Afsluitend presenteren we hier een kort stappenplan voor camerasystemen.

1. Bepaal het doel en de exacte werking van de camera's
Maak een analyse van het probleem en kies een doel. Doe dat zo precies mogelijk. Voor het tegengaan van inbraken of diefstallen is een ander cameraplan nodig dan voor het vergroten van het veiligheidsgevoel of het monitoren van patiënten. Werk exact uit *hoe* camera's moeten werken. Betrek zo snel collega's met verstand van privacy, medisch beroepsgeheim, ethiek, medezeggenschap en informatiebeveiliging.

2. Beoordeel de noodzakelijkheid
Camera's hebben soms voordelen, maar ze maken ook een inbreuk op de privacy. Dat mag alleen als het echt noodzakelijk is om camera's te gebruiken. Maak de afweging of de camera's in een goede verhouding staan tot het doel dat u wilt bereiken. Schiet nooit met een kanon op een mug: hou het zo klein mogelijk. Onderzoek of er lichtere alternatieven dan camera's zijn waarmee het doel ook kan worden bereikt. Denk aan sloten, verlichting, fysiek toezicht, bouwkundige beveiliging.

3. Maak een cameraplan
Bepaal hoeveel camera's u precies nodig hebt en waar u ze wilt plaatsen: een cameraplan. Dat kunt u direct met een cameraleverancier doen, maar het kan verstandig zijn eerst een onafhankelijk adviseur in de arm te nemen. Daarmee kunt u vrijuit alle opties bespreken en pas daarna offertes opvragen bij cameraleveranciers.

4. Doe uw juridische huiswerk
Stel een Data Protection Impact Assessment op. Onderbouw de noodzaak, maak de afweging tussen de belangen van het ziekenhuis en van anderen. Ga in op informatiebeveiliging. Zorg dat er verwerkersovereenkomsten worden gesloten met leveranciers en laat ze geheimhoudingsverklaringen ondertekenen. Betrek de ondernemingsraad en laat medewerkers meedenken.

Informeer iedereen over de camera's en zorg dat mensen hun rechten kunnen uitoefenen. Zorg dat taken, verantwoordelijkheden en rechten met betrekking tot beeldopnames voor alle betrokkenen duidelijk zijn.

5. Installeer en evalueer
Installeer het camerasysteem en bekijk na een paar weken of het systeem functioneert als bedoeld. Pas het indien nodig direct aan. Voer daarnaast periodiek een evaluatie uit om te zien of de camera's hebben gebracht wat u hoopte. Ja? Ontkurk de champagne! Nee? Ga terug naar het begin van dit stappenplan.

TIP Het toevoegen van meer camera's helpt meestal niet om een slecht functionerend camerasysteem te verbeteren.

Verder lezen

Regels cameratoezicht voor organisaties (Autoriteit Persoonsgegevens)
https://www.autoriteitpersoonsgegevens.nl/themas/cameratoezicht/cameratoezicht-bij-organisaties/regels-cameratoezicht-voor-organisaties

Beleidsregels cameratoezicht (Autoriteit Persoonsgegevens)
https://wetten.overheid.nl/BWBR0037591/2016-02-02#:~:text=De%20beleidsregels%20vormen%20een%20uitwerking,handhaving%20van%20de%20openbare%20orde

ICT&health – kennisplatform voor zorginnovatie
https://icthealth.nl/?s=camera

Adviesfunctie verantwoord datagebruik – meervoudig cameragebruik
https://realisatieibds.pleio.nl/wiki/view/ece7409e-f659-4127-99ef-3547306657e5/advies-meervoudig-gebruik-camerabeelden

Bodycams: Handreiking inzet bodycams in ziekenhuizen
https://www.staz.nl/wp-content/uploads/2021/06/Handreiking-gebruik-bodycams-StAZ-Veiligezorg.pdf

Drones – Europese regels
https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulations-eu

Model verwerkersovereenkomst van de Brancheorganisaties Zorg
https://www.vgn.nl/nieuws/boz-modelverwerkersovereenkomst-vernieuwd

Model verwerkersovereenkomst gemeenten (VNG)
https://www.informatiebeveiligingsdienst.nl/product/handreiking-standaard-verwerkersovereenkomst-gemeenten/

Opnemen van gesprekken door patiënten; Handreiking voor artsen (KNMG)
https://www.privacyindezorg.nl/assets/files/KNMG-handreiking-Opnemen-van-gesprekken-door-patiënten-(2017).pdf

Videoconsulten met patiënten (KNMG)
https://www.knmg.nl/actueel/nieuws/nieuwsbericht/alles-wat-u-moet-weten-over-videoconsulten-met-patienten

Advies over camera's in ziekenhuizen (België)
https://www.despecialist.eu/nl/nieuws/beroepsnieuws/camera-s-in-ziekenhuis-wat-mag-orde.html

Dankwoord

De auteur wil graag iedereen die heeft meegewerkt aan deze handreiking bedanken. Zij zijn werkzaam bij de volgende organisaties:

Amphia Breda
Amsterdam UMC
Catharina Ziekenhuis Eindhoven
CWZ Nijmegen
LUMC Leiden
OLVG Amsterdam
Openbaar Ministerie Oost-Nederland
Politie Amsterdam
Politie Oost-Nederland
UMCG Groningen
Zuyderland Heerlen

StAZ
Stichting
Arbeidsmarkt
Ziekenhuizen

Opgesteld door
Sander Flight Onderzoek & Advies

In opdracht van
Veiligezorg

Datum
5 juni 2024

Veiligezorg

Nederlandse Vereniging van Ziekenhuizen

FNV Zorg & Welzijn

CNV Zorg & Welzijn

FBZ vakbond voor zorgprofessionals

NU'91 voor zorgprofessionals