


① *Filip Goyens, data protection officer*
② *Inge Michielsens, juriste*

Nieuwe wetgeving zet puntjes op de i

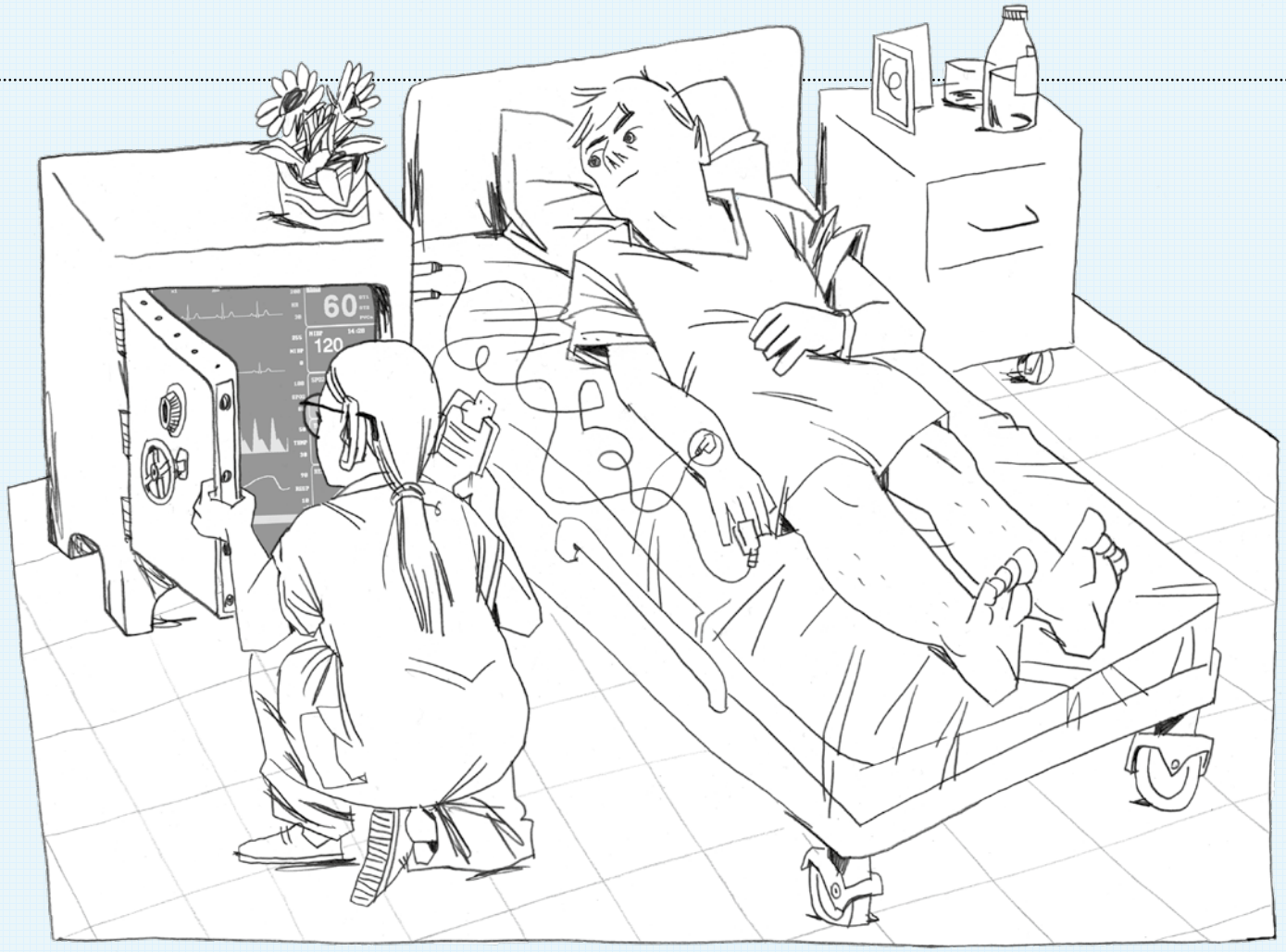
Uw gegevens in veilige handen

Een ziekenhuis houdt heel wat persoonlijke en medische gegevens van patiënten bij. Hoe zorgt het UZA ervoor dat die gevoelige informatie in veilige handen blijft?

Een patiënt die zich voor het eerst in het UZA aanmeldt, laat zijn identiteitskaart inlezen. Die persoonsgegevens zijn het vertrekpunt, zowel voor het medisch dossier, als voor de facturatie enzovoort. Naarmate er dan raadplegingen en onderzoeken gebeuren, komen er in het medisch dossier van de patiënt allerlei gegevens bij, soms tot genetische informatie toe. De privacywetgeving bepaalt hoe een ziekenhuis als het UZA met die gegevens om moet gaan. Recent werd die wetgeving strenger, via een Europese verordening – de Algemene Verordening Gegevensbescherming (AVR) of General Data Protection Regulation (GDPR) in het Engels. Tijd voor een gesprek met Filip Goyens, data protection officer in het UZA, en juriste Inge Michielsens.

Voor een ziekenhuis is omgaan met gevoelige gegevens niet nieuw. Hoe beveiligt het UZA die informatie?

‘De bescherming van de privacy van onze patiënten heeft altijd al voorop gestaan. Onze ICT-netwerken en -toepassingen zijn beveiligd volgens de strengste veiligheidsnormen. We laten ook periodiek onze netwerkbeveiliging testen door een extern bedrijf, om na te gaan of er toch geen hiaten in zitten. Een tweede belangrijk punt is natuurlijk



dat informatie nooit verloren mag gaan. Daarvoor maken we de nodige back-ups. In een ziekenhuis moet alle informatie echter zeven dagen op zeven de klok rond beschikbaar zijn. We kunnen het systeem dus niet eventjes stilleggen om onderhoud te doen. Daarnaast is de allereerste stap natuurlijk fysieke beveiliging: alle ruimtes waar geen patiënten en bezoekers mogen komen, dus ook ruimtes waar servers en dergelijke staan, zijn beveiligd via een badge-systeem.'

Heeft elke UZA-medewerker toegang tot alle informatie?

'Nee, absoluut niet. Om toegang te krijgen tot een medisch dossier of een medische toepassing heb je altijd een persoonlijke login en wachtwoord nodig. Elke medewerker krijgt alleen de toegangsrechten die hij nodig heeft. Een arts kan bijvoorbeeld in een medisch dossier meer doen dan een verpleegkundige. In het algemeen hebben medewerkers enkel toegang tot de patiëntendossiers waar zij bij betrokken zijn: er moet altijd sprake zijn van een therapeutische relatie. Bovendien houdt het systeem ook bij wie wanneer een dossier raadpleegt. Oneigenlijk gebruik van de gebruikersaccount van iemand anders is niet toegelaten en zelfs strafbaar.'

Naast de technologische aspecten is er ook een belangrijk menselijk aspect?

'Ja, informatieveiligheid en goed omgaan met persoonsgegevens is een taak van iedereen. Daarom geef je bijvoorbeeld je wachtwoord niet door aan een collega. De GDPR-regelgeving heeft op heel wat vlakken de puntjes op de i gezet en via infosessies werken we aan meer bewustwording bij al onze medewerkers. Volgens de nieuwe wetgeving is zelfs iemands gegevens zien of horen al een vorm van verwerking, waarvoor dus strenge regels gelden. Daarom moeten we ervoor zorgen dat er aan een balie niemand zomaar kan meelezen op een scherm.'

De nieuwe regelgeving vraagt om meer transparantie naar de patiënt toe over wat er met zijn gegevens gebeurt?

'Ja, de patiënt kan niet alleen zijn medisch dossier opvragen en binnenkort ook online raadplegen, hij heeft ook het recht om te weten welke artsen of andere medewerkers zijn medisch dossier hebben geraadpleegd. Daarnaast zijn we verplicht om patiënten te informeren over wat we precies doen met zijn of haar gegevens. Dat verloopt via de formulieren voor geïnformeerde →

→ toestemming die patiënten ondertekenen bij inschrijving of bij een onderzoek of ingreep. Die zullen expliciet vermelden welke gegevens we voor welke doeleinden gebruiken.'

Intussen delen ziekenhuizen en artsen ook steeds meer dossiers met elkaar. Hoe beveilig je de informatie in dat geval?

'De platformen die dat mogelijk maken, moeten aan dezelfde strenge veiligheidsvoorwaarden voldoen als de systemen binnen de ziekenhuizen. Wij werken via het CoZo-platform. Als een UZA-patiënt in een ander ziekenhuis terechtkomt, kan de arts daar via CoZo gegevens raadplegen. Belangrijk is dat de gegevens zelf niet verzonden worden. Die blijven hier in de beveiligde omgeving van het UZA, maar zijn via CoZo wel zichtbaar, eveneens via een beveiligde weg. Zo verklein je het risico dat er onderweg iets mee gebeurt.'

Heel wat UZA-diensten maken vandaag al gebruik van apps, vaak op mobiele toestellen, om patiënten op te volgen. Hoe hou je dat veilig?

'Bij dergelijke mobiele gezondheids-toepassingen sturen patiënten vanop afstand gegevens door naar het UZA. Ook daar nemen we de nodige maatregelen om te vermijden dat die persoonsgegevens gelekt of gehackt worden. Als een afdeling met zo'n app wil werken, vragen ze aan ons om een risicoanalyse te doen. We kunnen de leveranciers dan ook bepaalde eisen opleggen.'

Met steeds meer toepassingen en steeds strengere wetgeving, gaan er dan ook meer middelen naar ICT en informatieveiligheid?

'Beveiliging is altijd al een essentieel aspect geweest in de ICT, maar naarmate meer toepassingen digitaal worden en de beveiligingseisen strenger worden, heeft dat zeker ook een impact op de budgetten. Een veilig netwerk vraagt nu eenmaal de nodige investeringen. Ons team bestaat momenteel uit 65 mede-werkers, en die zijn ook steeds meer bezig met privacy. Door de strengere wetgeving is privacy een aandachtspunt vanaf de ontwikkeling van een nieuwe toepassing. *Privacy by design* noemen we dat. Het nieuwe elektronische patiëntendossier dat op komst is, is het beste voorbeeld. Van bij de start staan veiligheid en beveiliging voorop, terwijl het tegelijk vlot toegankelijk moet zijn voor de patiënt en de betrokken externe zorgverleners.' ⊙

Informatieveiligheid en goed omgaan met persoonsgegevens is een taak van iedereen.