



UMC Utrecht

Samenvatting

Reacties UMC's op OVV-rapport: 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen'



Rapport 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen'

RAPPORT

De Onderzoeksraad voor Veiligheid (OvV) heeft in februari 2020 een rapport over '*Patiëntveiligheid bij ICT-uitval in ziekenhuizen*' uitgebracht naar aanleiding van een aantal grote ICT-verstoringen binnen ziekenhuizen. Ook de verstoring op locatie Vumc van 23 oktober 2019 is hierbij onderzocht.

TIJDLIJNEN

- Onderzoek in 2019 door de Onderzoeksraad voor Veiligheid
- 1^e reactie NFU op hoofdlijnen gegeven door NFU/AcZie gezamenlijk
- Rapport uitgebracht in februari 2020
- Besproken in de AcZie van maart / april 2020
- UMC's nemen aanbevelingen over april / mei (zie volgende pagina)
- UMC's werken actieplannen uit juni / september
- Delen van de actieplannen in AcZie december 2020
- Delen van de actieplannen in de S&F januari 2021

CONCLUSIE

In alle UMCs is uitgebreid de stand van zaken rondom de aanbevelingen bekeken. Daarnaast is in een aantal huizen geconstateerd dat er naast deze aanbevelingen nog andere zaken aandacht behoeven. In de bijlagen zijn de assessments van de 7 UMCs opgenomen met actieplannen. Afsproken is dat deze binnen de UMCs zelf gemonitord zullen worden.



Het Rapport bevatte de volgende 4 aanbevelingen :

1. ICT-AFHANKELIJKHEID BINNEN ZORGPROCESSEN

De zorgverlening in ziekenhuizen is door de digitalisering dermate afhankelijk geworden van ICT dat grootschalige ICT-uitval kan leiden tot onveilige situaties voor patiënten. Voor een goede en veilige behandeling van patiënten is het van belang dat ziekenhuizen de afhankelijkheden van ICT binnen (zorg)processen in kaart brengen.

2. VOORKOMEN, BESTRIJDEN EN BEHEERSEN GEVOLGEN ICT-UITVAL

Voorkomen van ICT-uitval vereist een goede inrichting en beheer van het ICT-fundament. Het voorkomen van uitval, het vermogen om storingen snel te kunnen verhelpen als deze zich toch voordoen en het beheersen van de gevolgen ervan vraagt daarnaast om een goede voorbereiding. Onvolkomenheden in gemaakte keuzes bij de inrichting en het beheer van het ICT-fundament, alsmede bij de voorbereiding op ICT-uitval, hebben bijgedragen aan het langdurig uitvallen van de ICT bij de onderzochte voorvallen.

3. GEVOLGEN VAN ICT-UITVAL VOOR DE PATIËNTVEILIGHEID

De OvV onderscheidt 7 manieren waarop ICT-uitval tot schade aan patiënten kan leiden. Tijdens de ICT-storingen stond patiëntveiligheid in de afwegingen van professionals en managers steeds voorop. Na afloop van de storingen wordt echter nauwelijks systematisch nagegaan wat de gevolgen zijn geweest. Ziekenhuizen baseren hun antwoord op de vraag of de patiëntveiligheid tijdens de ICT-uitval in het geding is geweest hoofdzakelijk op daadwerkelijk opgetreden schade en niet op het ontstaan van onveilige situaties voor de patiënt. Na afloop van incidenten wordt niet of met weinig diepgang gekeken naar de gevolgen van de ICT-uitval voor de patiëntveiligheid. Ziekenhuizen noch andere partijen in het veld hebben een beeld van eventuele schade die is ontstaan doordat patiënten naar een ander ziekenhuis moesten uitwijken.

4. NOODZAAK VAN BESTUURLIJKE AANDACHT VOOR ICT-UITVAL

Bestuurlijke aandacht voor de risico's van ICT-uitval en de gevolgen daarvan voor de patiëntveiligheid is onontbeerlijk voor een adequate beheersing van die risico's. Daarbij zouden vooral de punten uit de voorgaande drie deelconclusies aandacht moeten krijgen. Ook is een gedeeld risicobesef onder medewerkers van belang en zouden de werelden van zorg en ICT nader bij elkaar gebracht moeten worden met het oog op het tijdig onderkennen van de risico's op ICT-uitval en de mogelijke gevolgen daarvan voor goede en veilige zorg.



Bijlagen

- Amsterdam UMC
- Erasmus MC
- LUMC
- MUMC
- Radboud UMC
- UMC Groningen
- UMC Utrecht



	Aanbeveling	Stand van zaken Amsterdam UMC
1a	Met het oog op een goede voorbereiding op uitval van ICT, de afhankelijkheden tussen zorg en ICT periodiek in kaart brengen, inclusief de mogelijke risico's voor patiënten die gepaard gaan met ICT-uitval.	Onder verantwoordelijkheid van de Medische Directie zijn uitgebreide plannen uitgewerkt voor diverse calamiteiten. Ook de uitval van centrale ICT-voorzieningen, evenals de uitval van telecom-voorzieningen, maken hier onderdeel van uit.
1b	Periodiek de ICT-systemen in samenhang testen, om te borgen dat de kritische zorgprocessen onder alle omstandigheden blijven functioneren. Ook dient geoefend te worden met scenario's waarbij de ICT in het ziekenhuis uitvalt. Betrek daar waar zinvol de leveranciers bij deze oefeningen en testen.	Het inplannen van een uitgebreide disaster & recovery test m.b.t. EPIC was in 2020 niet goed mogelijk. Het vanwege een test tijdelijk niet beschikbaar zijn van EPIC is vanuit het perspectief van zorgverleners vaak lastig. Wel wordt jaarlijks meegedaan met OZON waarbij een calamiteit in de vorm van een scenario-oefening moet worden aangepakt.
1c	Na elke ernstige ICT-uitval evaluaties uitvoeren waarbij ook de (verhoogde kans op) schade voor zowel de patiënten in het ziekenhuis als voor de uitgeweken patiënten diepgaand wordt geanalyseerd. Betrek daarbij waar nodig de partners in de zorgketen.	Het uitvoeren van evaluaties maakt standaard onderdeel uit van de crisisorganisatie die wordt geactiveerd bij ernstige ICT-verstoringen. Onder verantwoordelijkheid van de medische directie gebeurt dat in het algemeen grondig en systematisch. Verbeterpunten worden ook gevolgd. Er zou wellicht meer aandacht kunnen worden besteed aan eventuele schade voor eventueel uitgeweken patiënten.
1d	Over alle drie de hierboven genoemde aspecten jaarlijks publiek verantwoording afleggen.	ICT-verstoringen worden opgenomen in een integrale kwartaalrapportage over Incidenten, Bedrijfsongevallen en Onveilige Situaties. Deze worden besproken in de RvB en zijn toegankelijk.
2	Borg dat ziekenhuizen dit vraagstuk gezamenlijk benaderen en van en met elkaar leren.	Grote ICT-verstoringen worden in UMC verband besproken. Dit gebeurt in TacZie en in AcZie met als doel om kennis te delen en te kijken op welke wijze kan worden samengewerkt.
3	Ontwikkel een praktisch handvat voor ziekenhuizen voor het beheersen van de risico's van uitval van ICT, waarin de in dit rapport genoemde aanknopingspunten worden meegenomen.	Op twee manieren wordt binnen Amsterdam UMC invulling gegeven aan deze aanbeveling. De Medische Directie heeft de calamiteitenprocedures en –plannen bijgewerkt en de Dienst ICT werkt - als onderdeel van de maatregelen in het kader van NEN7510 – met een gedetailleerde risicomanagementrapportage. In deze rapportage wordt input van verschillende kanten samengebracht: vervolgcacties uit eerdere incidenten, bevindingen uit uitgevoerde audits, risico's die door beheerders zijn opgemerkt, et cetera.

Aanbevelingen veiligheidsraad

Aanbeveling	Stand van zaken UMCUtrecht
<p>1a Met het oog op een goede voorbereiding op uitval van ICT, de afhankelijkheden tussen zorg en ICT periodiek in kaart brengen, inclusief de mogelijke risico's voor patiënten die gepaard gaan met ICT-uitval.</p>	<p>Voor het belangrijkste zorg-systeem (HiX) is een calamiteitenplan beschikbaar waarin de risico's beschreven zijn en mogelijke scenario's uitgewerkt zijn.</p> <p>Daarnaast is er een noodprocedure beschikbaar, waardoor bij uitval de belangrijkste patiënt gegevens beschikbaar zijn. Dit gaat door middel van meer dan 100 dedicated nood-PC's, die zonder netwerk kunnen functioneren en waarbij elke nacht de meest recente gegevens van patiënten uit HiX worden opgeslagen en gebruikt kunnen worden.</p>
<p>1b Periodiek de ICT-systemen in samenhang testen, om te borgen dat de kritische zorgprocessen onder alle omstandigheden blijven functioneren. Ook dient geoefend te worden met scenario's waarbij de ICT in het ziekenhuis uitvalt. Betrek daar waar zinvol de leveranciers bij deze oefeningen en testen.</p>	<p>Grote testen worden beperkt in samenhang uitgevoerd. Dit jaar zou zo'n test plaatsvinden (OZON) maar is uitgesteld i.v.m. corona. Wel wordt regelmatig getest:</p> <ul style="list-style-type: none"> - Recovery testen - Back-up testen
<p>1c Na elke ernstige ICT-uitval evaluaties uitvoeren waarbij ook de (verhoogde kans op) schade voor zowel de patiënten in het ziekenhuis als voor de uitgeweken patiënten diepgaand wordt geanalyseerd. Betrek daarbij waar nodig de partners in de zorgketen.</p>	<p>Bij elke calamiteit en grote storing wordt direct met gebruikers van de systemen gecommuniceerd.</p> <p>Waar nodig vindt opschaling plaats naar de crisis-organisatie van het UMC Utrecht, waarin o.a. de RvB vertegenwoordigd is. Na elke grote storing vindt een uitgebreide evaluatie plaats met alle betrokkenen.</p> <p>Op basis hiervan worden verbetervoorstellen gedaan en uitgevoerd.</p>
<p>1d Over alle drie de hierboven genoemde aspecten jaarlijks publiek verantwoording afleggen.</p>	<p>Vanuit ICT wordt per kwartaal een rapportage gemaakt voor de Raad van Bestuur en Raad van Toezicht. Deze is na behandeling inzichtelijk.</p>
<p>2 Borg dat ziekenhuizen dit vraagstuk gezamenlijk benaderen en van en met elkaar leren.</p>	<p>Grote storingen worden in UMC verband besproken. Zie voorbeeld Maastricht 'gijzeling'.</p> <p>Maandelijks komen zowel de CIO's als de managers Infrastructuur van alle UMC's afzonderlijk bijeen waar gezamenlijke onderwerpen worden besproken. Hier wordt kennis uitgewisseld en worden afspraken over samenwerking mbt een heel scala aan onderwerpen gemaakt.</p>
<p>3 Ontwikkel een praktisch handvat voor ziekenhuizen voor het beheersen van de risico's van uitval van ICT, waarin de in dit rapport genoemde aanknopingspunten worden meegenomen.</p>	<p>Binnen het UMC Utrecht is risicomanagement 2 jaar geleden op een beperkt aantal IT-aspecten gestart. Er wordt nu een project opgezet binnen het UMC Utrecht, wat in 2021 moet leiden tot concreet risicomanagement. Het eerste aandachtspunt is het primaire proces.</p> <p>Dit leidt tot een praktisch handvat voor het UMC Utrecht en kan gedeeld worden met andere ziekenhuizen of besproken in NFU verband.</p>
<p>4 Ga in regionaal verband na of in geval van ICT-uitval waarbij meerdere ziekenhuislocaties in een regio worden getroffen, de veiligheid van patiënten voldoende is geborgd.</p>	<p>Als er langdurige, evt. regionale ICT-uitval is, wordt de crisisorganisatie van het UMC Utrecht in stelling gebracht. Door de noodprocedure zijn de belangrijkste gegevens van patiënten beschikbaar. Als de veiligheid van patiënten in het geding komt, zal worden gekeken of patiënten kunnen worden overgeplaatst naar andere ziekenhuizen, evt. buiten de regio. Dit wordt aangestuurd vanuit de crisisorganisatie, waar ook ICT in participeert.</p> <p>Daarnaast heeft het UMC Utrecht het 'noodhospitaal' wat door andere ziekenhuizen in geval van calamiteiten gebruikt zou kunnen worden. (Zo werd dit bv in 2015 gebruikt voor 95 patiënten die vanuit het VUMC werden verhuisd als gevolg van ondergelopen kelders aldaar.) ICT voor de tijd in het noodhospitaal is geregeld, maar of gebruik gemaakt kan worden van gegevens uit het eigen ziekenhuis- dossier is afhankelijk van de wijze waarop het andere ziekenhuis de gegevens beschikbaar hebben.</p>

