

Bijlage E

Analyse crisisbeheersing

Den Haag, februari 2020

De rapporten van de Onderzoeksraad voor Veiligheid zijn openbaar en te vinden op onderzoeksraad.nl.

De Onderzoeksraad heeft onderzoek gedaan naar de ICT-storingen in het Radboudumc, het IJsselland Ziekenhuis en het Dijklander Ziekenhuis. Het onderzoek naar de crisisbeheersing is uitgebreid weergegeven in deze bijlage.

LIJST VAN AFKORTINGEN

BHV	Bedrijfshulpverlening
CBT	Crisisbeleidsteam
CC	Calamiteitencoördinator
IC	<i>Intensive Care</i>
ICM	Integraal Crisismanagement
ICP	Integraal Crisisplan
ICT	Informatie- en communicatietechnologie
OCT	Operationeel Crisisteam
OT	Operationeel Team
OTO	Opleiden, trainen en oefenen
RvB	Raad van bestuur
SEH	Spoedeisende Hulp
ZiROP	Ziekenhuis Rampen Opvang Plan

LIJST VAN BEGRIPPEN

Controller (storage)

Een element in een storagestelsel dat de functie heeft om data weg te schrijven en op te halen van de opslagdisks van de storage.

Crisisplan

Een samenhangend plan waarin een basiswerkwijze staat beschreven voor crisissituaties en waarin een relatie naar onderliggende plannen en procedures is vastgelegd. Hierbij gaat het niet alleen over crisissituaties die de continuïteit van zorg bedreigen, maar over alle soorten crises die een organisatie kunnen raken. Een crisisplan komt niet in de plaats van bestaande plannen (zoals een ziekenhuis rampen opvangplan of continuïteitsplan), maar verbindt deze plannen en zorgt daarmee voor onderlinge samenhang tussen de plannen en procedures. Het biedt een basis om op elke crisis voorbereid te zijn.

Informatiemanagement

Binnen crisisbeheersing betreft informatiemanagement het proces van (onder andere) het verzamelen, valideren en het verspreiden van operationele informatie, evenals de vastlegging van alle relevante informatie tijdens de crisisbeheersing.

Failover

De overschakeling van de primaire node naar de secundaire node.

Ziekenhuis Rampen Opvang Plan (ZiROP)

Een (verplicht) plan waarin beschreven staat wie wat moet doen in het geval van ongevallen en rampen (buiten het ziekenhuis).

E.1 Radboudumc

E.1.1 Visie en planvorming

Het Radboudumc heeft de voorbereiding op calamiteiten, crises en rampen vastgelegd in het *Crisis- en Calamiteitenplan Radboudumc*. Dit is een integraal crisisplan¹, gericht op zowel externe incidenten (waarbij het Radboudumc slachtoffers opvangt en behandelt) als interne incidenten.² De meest recente versie van dit plan dateert van november 2016 en is geautoriseerd door de raad van bestuur (RvB). Het plan wordt iedere twee jaar herijkt.

In aanvulling op dit plan bestaan deelplannen voor Radboudumc-brede processen bij crises en calamiteiten (bijvoorbeeld over familie- en verwantenopvang en ontruiming van gebouwen) en afdelingscalamiteitenplannen met specifieke informatie over hoe afdelingen kunnen functioneren tijdens een calamiteit of crisis.³ Uit de, op verzoek van de Raad, aangeleverde calamiteitenplannen van de Spoedeisende Hulp (SEH), de Intensive Care (IC) en het laboratorium blijkt dat de SEH geen specifiek plan heeft om de continuïteit van de dienstverlening bij uitval van ICT-voorzieningen te borgen.⁴ Bij de andere twee afdelingen is zo een plan wel uitgewerkt, maar de diepgang hiervan verschilt onderling sterk. Dit kan mogelijk verklaard worden, doordat de afdeling zelf verantwoordelijk is voor de kwaliteit en actualiteit van de plannen, zonder dat hier centraal toezicht/controlle op is.

E.1.2 Risicoanalyse

Aan het *Crisis- en Calamiteitenplan Radboudumc* ligt een risicoprofiel ten grondslag, bestaande uit de externe en interne rampen en calamiteiten waarop het Radboudumc zich voorbereidt. Eén van de onderscheiden risico's in het risicoprofiel is een uitval van informatievoorzieningen. Dit risico is ingeschaald als ernstig (qua impact) en zeer waarschijnlijk (qua kans). In het *Crisis- en Calamiteitenplan Radboudumc* is aangegeven dat dit risico (net als de andere belangrijke risico's) zal worden uitgewerkt. Dit is ook aanbevolen in een in 2018 gepubliceerde scan van de crisisbeheersing van het

1 Een crisisplan is samenhangend plan waarin een basiswerkwijze staat beschreven voor crisissituaties en waarin een relatie naar onderliggende plannen en procedures is vastgelegd. Hierbij gaat het niet alleen over crisissituaties die de continuïteit van zorg bedreigen, maar over alle soorten crises die een organisatie kunnen raken. Een crisisplan komt niet in de plaats van bestaande plannen (zoals een ziekenhuis rampen opvangplan of continuïteitsplan), maar verbindt deze plannen en zorgt daarmee voor onderlinge samenhang tussen de plannen en procedures. Het biedt een basis om op elke crisis voorbereid te zijn.

2 Radboudumc, 2016, *Crisis- en Calamiteitenplan Radboudumc 2016*, pagina 2.

3 Radboudumc, 2016, *Crisis- en Calamiteitenplan Radboudumc 2016*, pagina 4.

4 Radboudumc, 2016, *Rampenslachtoffers in de acute keten en Radboudumc, 2017, Rampenslachtoffers in de acute keten – spoed eisende hulp*.

Radboudumc.⁵ Dit onderzoek is in opdracht van het ziekenhuis door een externe partij uitgevoerd.⁶ Zowel het voorschrift in het crisisplan als de aanbeveling van de externe partij heeft tot op heden niet geleid tot een concrete uitwerking van dit risico. Het Radboudumc beschikte wel over een zogenaamde scenariokaart voor dit risico, die de crisisorganisatie in algemene termen aandachtspunten geeft over hoe te handelen in de warme fase bij optreden van dit risico. Dit is echter niet een plan dat de crisisorganisatie concreet voorbereidt op dit risico en hoe dit het beste kan worden bestreden in het Radboudumc.

E.1.3 Melden en alarmeren

In het *Crisis- en Calamiteitenplan Radboudumc* is het proces voor melding en alarmering beschreven. Hierbij is een apart proces beschreven voor een incident waarbij infrastructurele of informatievoorzieningen, zoals ICT, zijn verstoord of uitgevallen. De melding en alarmering in het Radboudumc verliep tijdens de ICT-storing van 26 januari 2018 op hoofdlijnen conform de processen die zijn beschreven in het crisisplan.

E.1.4 Op- en afschalen

In het *Crisis- en Calamiteitenplan Radboudumc* is het proces voor op- en afschaling beschreven. Daaruit blijkt dat de calamiteitencoördinator (CC) of de voorzitter van het crisisbeleidsteam (CBT) bepaalt of er sprake is van een calamiteit.⁷ De voorzitter van het CBT bepaalt daarbij of naar crisismanagement overgeschakeld moet worden en het CBT bijeen dient te komen. De voorzitter CBT bepaalt uiteindelijk ook of een calamiteit is afgelopen en of het crisismanagement kan worden opgeheven. Dat doet hij in overleg met de RvB. De op- en afschaling in het Radboudumc verliep tijdens de ICT-storing van 26 januari 2018 op hoofdlijnen conform de processen die zijn beschreven in het crisisplan. Er is relatief snel afgeschaald nadat de ICT-storing was afgelopen. Dit leidde niet tot problemen voor (zorg)afdelingen in het ziekenhuis.

E.1.5 Leiding en coördinatie

In de planvorming van het Radboudumc is de leiding en coördinatie tijdens de crisisbeheersing helder belegd. De voorzitter CBT heeft daarbij een centrale rol, bijgestaan door een CC en een persvoorlichter. Er is daarmee sprake van een compacte kern, die flexibel kan worden uitgebreid met andere specialisten. De RvB blijft altijd eindverantwoordelijk voor de crisisbeheersing. Tijdens de ICT-storing van 26 januari 2018 verliep de leiding en coördinatie op hoofdlijnen conform de structuur uit het crisisplan. De CC speelde een voornamelijk rol in de beeldvorming over het incident. In de door de voorzitter CBT voorgezeten vergaderingen van het CBT vond de oordeelsvorming plaats en de voorzitter CBT nam in overleg met de RvB de besluiten over de crisisbeheersing.

5 Helsloot en Kijne, 2018, *Scan crisisorganisatie Radboudumc*, pagina 4.

6 De opdracht voor deze scan is in 2017 gegeven.

7 Radboudumc, 2016, *Crisis- en Calamiteitenplan Radboudumc 2016*, pagina 13.

E.1.6 Informatiemanagement

In het *Crisis- en Calamiteitenplan Radboudumc* is geen proces opgenomen voor informatiemanagement⁸. Ook uit de interviews met mensen uit de crisisorganisatie is niet gebleken dat zo een proces binnen het Radboudumc aanwezig is. Het is daardoor niet duidelijk op welke manier informatie dient te worden verzameld tijdens een calamiteit of crisis en op welke manier deze informatie wordt gedeeld binnen de crisisorganisatie. Ook de borging van informatie en besluiten door middel van gestandaardiseerde verslaglegging in CBT-overleggen is niet via een proces ingeregeld.

Dit leidde ertoe dat de CC in de eerste uren van de ICT-storing van 26 januari 2018 moeite had om de impact voor het ziekenhuis goed in beeld te krijgen door de grote hoeveelheid informatie die hij moest verwerken. Indien sprake was geweest van een goed gestructureerd proces voor informatiemanagement, had dit beter kunnen verlopen. Het is bovendien onduidelijk of en hoe de informatie die werd gedeeld in het CBT op een gestructureerde manier werd vastgelegd. Ten tijde van dit onderzoek bleken namelijk geen verslagen van de overleggen van het CBT en het operationeel team (OT) ICT beschikbaar. Betrokkenen geven aan dat er wel verslaglegging heeft plaatsgevonden door een student van de medische faculteit, maar het Radboudumc heeft deze verslagen niet aan kunnen leveren bij de Onderzoeksraad.

E.1.7 Crisiscommunicatie (intern)

Over het verspreiden van informatie over en tijdens een calamiteit of crisis naar de rest van de organisatie, oftewel de interne crisiscommunicatie⁹, is geen proces opgenomen in het *Crisis- en Calamiteitenplan Radboudumc*.

Tijdens de ICT-storing van 26 januari 2018 heeft de interne communicatie in het ziekenhuis plaatsgevonden via de belcomputer, via het intranet en via email. Ook is getracht medewerkers te informeren via het zogenoemde *Radboudumc-alert*; een systeem dat specifiek ontwikkeld is om in crisissituaties ingezet te worden om mensen te informeren.¹⁰ Het bleek dat juist dit crisiscommunicatiesysteem niet werkte tijdens de ICT-storing op 26 januari 2018, omdat het gebruik maakt van de reguliere ICT-systemen in het ziekenhuis.¹¹ Naar aanleiding hiervan heeft het Radboudumc inmiddels een (crisis) communicatietool ontwikkeld, die ook in het geval van een ICT-storing blijft functioneren.¹²

E.1.8 Opleiden, trainen en oefenen

Een belangrijk deel van de voorbereiding op een crisis of calamiteit is het opleiden, trainen en oefenen (OTO) van functionarissen in de crisisorganisatie. In het *Crisis- en*

8 Dit betreft (onder andere) het verzamelen, valideren en het verspreiden van operationele informatie, evenals de vastlegging van alle relevante informatie tijdens de crisisbeheersing.

9 Voor dit onderzoek is op het gebied van crisiscommunicatie alleen gekeken naar de interne crisiscommunicatie: in hoeverre is de verspreiding van de juiste, tijdige en begrijpelijke informatie binnen de organisatie geborgd door een proces dat in de voorbereiding is opgesteld.

10 Radboudumc-alert is een applicatie waarmee het mogelijk is om een bericht te sturen dat iedereen, die is ingelogd, als een pop-up op zijn of haar computerscherm krijgt.

11 Radboudumc, 2018, *Evaluatie inzet crisisorganisatie tijdens ICT storing 26 januari 2018*.

12 Radboudumc, 2018, *Evaluatie inzet crisisorganisatie tijdens ICT storing 26 januari 2018*.

Calamiteitenplan Radboudumc zijn de ambities, doelstellingen en verantwoordelijkheden voor het OTO-programma van het Radboudumc vastgelegd.¹³

Eén van de vastgelegde ambities is om de genoemde interne en externe risico's in het crisisplan als uitgangspunt te gebruiken voor de OTO-activiteiten. Dat betekent dat ook het risico op uitval van ICT aandacht zou moeten krijgen. Dat is immers als één van de belangrijkste risico's benoemd in het *Crisis- en Calamiteitenplan Radboudumc*. Uit verslagen van trainingen in 2017 en 2018 blijkt dat deze ambitie is waargemaakt voor (potentiële) OT ICT leden.¹⁴ Uit het OTO-programma 2018-2020 blijkt dat ook voor de komende jaren voorzien is in trainingen met ICT-scenario's voor (potentiële) OT ICT leden.¹⁵

In het programma is echter niet voorzien in OTO-activiteiten met een ICT-scenario voor de functionarissen in de crisisorganisatie, die op tactisch en/of strategisch niveau opereren. Uit interviews met deze functionarissen blijkt dat zij de afgelopen jaren geen trainingen hebben gevolgd waarin gebruik is gemaakt van een scenario waarbij de ICT uitvalt. Er is wel een grootschalige *table-top* oefening gehouden met het uitvallen van een nutsvoorziening (elektriciteit).

E.1.9 Evalueren

In het *Crisis- en Calamiteitenplan Radboudumc* zijn de richtlijnen gegeven voor de evaluatie van calamiteiten en crises.¹⁶ De Raad heeft alle rapportages van incidenten waarbij sprake was van verstoring, uitval en/of misbruik van ICT van de afgelopen tien jaar ontvangen van het Radboudumc. Hieruit blijkt dat al deze incidenten op enigerlei wijze zijn geëvalueerd en dat verbeterpunten zijn beschreven. Uit de ontvangen stukken en gesprekken met betrokkenen blijkt dat de verbeterpunten bovendien structureel worden opgevolgd en worden geïmplementeerd in de (crisis)organisatie. In de ontvangen rapportages is geen expliciete aandacht besteed aan de gevolgen van de storing voor de patiëntveiligheid.

Ook de ICT-storing van 26 januari 2018 is geëvalueerd. Hiervan is een evaluatierapport¹⁷ gemaakt, waarin de inzet van het crisismanagement en de verbeterpunten zijn opgenomen. In het rapport zijn dertien verbeterpunten benoemd, bestaande uit acht actiepunten en vijf tips voor de betrokkenen in de crisisorganisatie. De actiepunten zijn een paar maanden na het voorval (medio mei) afgerond.¹⁸ In de evaluatie is niet aangegeven wat de impact van de storing was op de patiëntveiligheid. Betrokkenen bij het voorval en de evaluatie geven aan dat er in hun beleving geen impact is geweest voor de patiëntveiligheid, maar dat dit niet expliciet onderbouwd is met een analyse op patiënt- of afdelingsniveau. Er is ook geen zicht op de gevolgen voor de mensen die onder normale omstandigheden zouden zijn opgenomen in het Radboudumc, maar daar door de algehele opnamestop tijdens de ICT-storing niet terecht konden.

¹³ Radboudumc, 2016, *Crisis- en Calamiteitenplan Radboudumc 2016*, pagina 18-19.

¹⁴ Radboudumc, 2018, *Rapport trainingen OT ICT voorjaar 2018 en Rapportage trainingen OT ICT mei 2017*.

¹⁵ Radboudumc, 2018, *OTO in schema 2018-2020*.

¹⁶ Radboudumc, 2016, *Crisis- en Calamiteitenplan Radboudumc 2016*, pagina 14.

¹⁷ Radboudumc, 2018, *Evaluatie inzet crisisorganisatie tijdens ICT storing 26 januari 2018*.

¹⁸ Radboudumc, 2018, *Evaluatie inzet crisisorganisatie tijdens ICT storing 26 januari 2018*.

Samenvattende conclusie

De crisisorganisatie van het Radboudumc heeft tijdens het incident de gevolgen voor de patiëntenzorg over het algemeen goed beheerst. Crisisfunctionarissen konden bij hun optreden terugvallen op een gedegen voorbereiding. Zo was er een integraal crisisplan beschikbaar en hebben ze OTO-activiteiten gevolgd. Wel ontbraken concrete handvatten voor het specifieke risico dat zich openbaarde: uitval van ICT-voorzieningen. Noch in de planvorming noch in de OTO-activiteiten is hier namelijk specifiek aandacht aan besteed. In de planvorming is ook geen aandacht voor het informatiemanagement tijdens een crisissituatie, wat er in de praktijk toe leidde dat het relatief lang duurde voordat de impact van de situatie goed in beeld was bij de crisisorganisatie. ICT-incidenten worden binnen het Radboudumc geëvalueerd. In de evaluaties wordt geen aandacht besteed aan de gevolgen voor de veiligheid van de patiënten in het ziekenhuis.

E.2 IJsselland ziekenhuis

E.2.1 Visie en planvorming

Het IJsselland Ziekenhuis beschikte ten tijde van het onderzoek niet over een integraal crisisplan. Dit was wel in ontwikkeling. Het integrale crisisplan, het zorgcontinuïteitsplan genoemd, zal het beleid, de procedures en de middelen die het ziekenhuis naar eigen inzicht nodig heeft om voorbereid te zijn op calamiteiten, noodsituaties en rampen beschrijven. Hierbij worden eerdere plannen, zoals de decentrale bedrijfshulpverleningsplannen, ZiROP¹⁹ en pandemieplannen, samengevoegd. Het wordt een integraal plan voor alle onderdelen en afdelingen van het IJsselland Ziekenhuis. De basis voor de crisisbeheersing in het IJsselland Ziekenhuis lag ten tijde van het voorval in het ZiROP.

Het eerste deel van het zorgcontinuïteitsplan was ten tijde van het onderzoek wel gereed en bestond uit een strategisch kader en een tactisch bedrijfshulpverleningsplan. Het strategisch kader geeft de visie op het gebied van veiligheid en zorgcontinuïteit voor een periode van drie jaar. Het is de leidraad om de voorzitter van de RvB te ondersteunen in zijn eindverantwoordelijkheid voor de veiligheid in het IJsselland Ziekenhuis. Het tactisch bedrijfshulpverleningsplan beschrijft in procedures hoe medewerkers van het ziekenhuis en onderhuurders binnen het ziekenhuisterrein moeten handelen in geval van een calamiteit of een (dreigende) noodsituatie. Het plan bevat basisinformatie over rollen, verantwoordelijkheden en afdelingsspecifieke informatie en is voor alle afdelingen gelijk. Beide documenten zijn in mei 2018 formeel vastgesteld door de voorzitter van de RvB.

¹⁹ Ziekenhuis Rampen Opvang Plan (ZiROP) is een (verplicht) plan waarin beschreven staat wie wat moet doen in het geval van ongevallen en rampen (buiten het ziekenhuis).

Elke (zorg)afdeling binnen het IJsselland Ziekenhuis heeft noodprocedures en noodformulieren op papier om op terug te vallen tijdens een ICT-storing. Noodprocedures zijn afdelingsspecifieke procedures die concreet voorschrijven hoe er gewerkt moet worden in afwijkende situaties, zoals bij uitval van ICT. De noodprocedures vormen geen onderdeel van het centrale overkoepelende zorgcontinuïteitsplan. Afdelingen zijn zelf verantwoordelijk voor de kwaliteit, de beschikbaarheid en het actueel houden van de eigen kennis en noodprocedures.²⁰

E.2.2 Risicoanalyse

Indien zich een calamiteit voordoet, moet er een juiste inschatting worden gemaakt van de aard, ernst en de omvang van de calamiteit om de juiste respons tot stand te brengen. Het strategisch kader benoemt dat voor deze fase er altijd een groot verschil zit tussen de beschikbare informatie en de informatiebehoefte om de juiste respons te kunnen bepalen. Het strategisch kader beschrijft daarom naast algemene risico's als brand en ongevallen ook meer specifieke veiligheidsrisico's, waaronder uitval van ICT²¹, en de omvang van de calamiteitenorganisatie en de scenario's om daarmee om te gaan. Omdat de hoeveelheid van denkbare veiligheidsrisico's te groot is om afzonderlijke draaiboeken en plannen voor te ontwikkelen, heeft het IJsselland Ziekenhuis ervoor gekozen zich voor te bereiden op zeven mogelijke gevolgen van een calamiteit²², waaronder 'Uitval nutsvoorzieningen, apparatuur en ICT-middelen'. De uitwerking hiervan is een instructie voor het CBT, het hoofd bedrijfshulpverlening (BHV), de coördinator BHV, de ploegleider BHV, BHV'ers en medewerkers.²³ Het beschrijft summier de melding, alarmering en besluitvormingsprocedure, maar geeft geen concreet overzicht van risico's en bijbehorende beheersmaatregelen die als handvat kunnen dienen voor de respons. Omdat niet alle denkbare situaties kunnen worden uitgewerkt, stelt het strategisch kader dat er 'een beroep wordt gedaan op het improvisatievermogen en het intuïtieve vermogen van het CBT en de weerbaarheid van de organisatie als geheel.'²⁴

E.2.3 Melden en alarmeren

Het IJsselland Ziekenhuis heeft een uitgewerkt algemeen proces voor melden en alarmeren voor verschillende soorten calamiteiten en crises, waaronder een summier instructie voor melden en alarmeren bij ICT-uitval. Deze beschrijving is opgenomen in het strategisch kader van het zorgcontinuïteitsplan. Hierin staat dat meldingen van incidenten gedaan moeten worden bij de receptie of bedrijfshulpverleningsorganisatie. Deze beslist op basis van vastgestelde procedures over alarmeren en informeren van de juiste functionarissen (hoofd BHV of de CC).²⁵

Op 3 juni 2018 is op hoofdlijnen gehandeld conform deze procedure. Medewerkers die hinder ondervonden van de storing hebben dit rond 01:20 uur gemeld bij de receptie. De receptionist maakte hiervan melding bij het dienstdoende avond-/nachthoofd en

²⁰ *Zorgcontinuïteitsplan, strategisch kader versie 6.0*, mei 2018, pagina 10.

²¹ *Zorgcontinuïteitsplan, strategisch kader versie 6.0*, mei 2018, scenario N; uitval ICT: Netwerk/EPD/telefonie.

²² *Zorgcontinuïteitsplan, strategisch kader versie 6.0*, mei 2018, zeven gevolgen van een calamiteit: verplaatsen van cliënten; uitval nutsvoorzieningen, apparatuur en ICT-middelen; sluiting van delen van de locatie; groot aanbod van cliënten; logistieke stagnatie; tekort aan personeel; uitbraak infectieziekten.

²³ *Zorgcontinuïteitsplan, strategisch kader versie 6.0*, mei 2018, pagina 17.

²⁴ *Zorgcontinuïteitsplan, strategisch kader versie 6.0*, mei 2018, pagina 15.

²⁵ *Zorgcontinuïteitsplan, strategisch kader versie 6.0*, mei 2018, pagina 10.

informeerde de dienstdoende ICT-medewerker. De dienstdoende ICT-medewerker constateerde na de eerste controles dat er sprake was van een netwerkstoring, maar kon niet vaststellen wat de oorzaak hiervan was. Daarmee had hij ook geen indicatie hoe lang de storing zou kunnen gaan duren. De ICT-medewerker besloot vervolgens na overleg met het dienstdoende avond-/nachthoofd om de CC in te lichten.

E.2.4 Op- en afschalen

Het IJsselland Ziekenhuis heeft een uitgewerkt opschalingsproces voor het CBT, waarin de verantwoordelijkheden duidelijk zijn belegd. Het hoofd BHV of de CC beslist in overleg met het dienstdoende lid van de RvB of en in welke mate wordt opgeschaald naar een CBT. De CC bepaalt aan de hand van het te verwachten letsel of de getroffen zorgafdelingen in een zo vroeg mogelijk stadium welke medisch specialist(en) aan het CBT moet(en) worden toegevoegd. Het CBT kan ook in een later stadium nog besluiten om (aanvullende) functionarissen uit een bepaald specialisme toe te voegen. Het CBT kan ook besluiten om een operationeel crisisteam (OCT) in te stellen om het CBT te ondersteunen, operationele taken uit te voeren en de interne aansturing van de organisatie te laten verzorgen. De aard van de calamiteit is dan bepalend voor het voorzitterschap van een OCT.

Tijdens de storing op 3 juni 2018 besloot de CC bijna direct nadat ze geïnformeerd was om op te schalen naar een CBT. Zij informeerde rond 01:45 uur de voorzitter van de RvB over de ICT-storing in het ziekenhuis. Deze informeerde rond 02:00 uur per telefoon het hoofd BHV. Daarmee waren de drie kernleden van het CBT geïnformeerd. In een eerste telefonische informatieronde tussen deze kernleden werd besloten om om 06:00 uur bij elkaar te komen in een CBT-overleg. In dit eerste CBT-overleg bleek geen zicht te zijn op herstel van de stabiliteit van de ICT-systemen en werd besloten de dienstdoende (weekend)artsen van alle kritische (zorg)afdelingen om 07:00 uur in huis te halen om te overleggen over de noodzakelijke maatregelen om de continuïteit van zorg en de veiligheid van patiënten te waarborgen.

De opschaling heeft hiermee plaatsgevonden langs de lijn die is beschreven in de planvorming. De Raad constateert wel dat met een volledige uitval van alle ICT-voorzieningen (rond 01:30 uur) er de facto sprake was van een crisissituatie die aansturing behoeft. Door pas om 06:00 uur als CBT bij elkaar te komen was de aansturing van de incidentbestrijding tot 06:00 uur niet optimaal. De gevolgen hiervan waren beperkt, omdat er gedurende de nacht weinig activiteit was in het ziekenhuis.

E.2.5 Leiding en coördinatie

Indien er wordt besloten tot het instellen van een CBT geldt er een afwijkende structuur voor leiding en coördinatie van alle activiteiten om de crisis of calamiteit te bestrijden en de gevolgen ervan te beheersen. Het CBT, met het dienstdoende lid van de RvB als CBT-voorzitter, geeft sturing aan de organisatie tijdens een calamiteit op bestuurlijk/strategisch niveau. De voorzitter CBT is verantwoordelijk voor de coördinatie van de gehele crisisbeheersing en de besluitvorming binnen het CBT, bepaalt op hoofdlijnen het beleid en coördineert interne- en externe communicatie. Hij laat zich standaard bijstaan door de CC (adviseur), het hoofd BHV, het hoofd van de Directie Informatievoorziening en Facilitaire Zaken en een communicatiemedewerker. Om de

vergaderingen gestructureerd te laten verlopen, wordt gebruik gemaakt van de BOBOC-systematiek.²⁶

De voorzitter van de RvB trad, conform het vooraf bedachte proces voor leiding en coördinatie, op 3 juni 2018 in het CBT op als voorzitter en heeft vanuit die rol de crisisbeheersing gecoördineerd. Door alle dienstdoende (weekend)artsen, inclusief de aanwezige AIOS en relevante medewerkers uit ondersteunende diensten, uit te nodigen voor het CBT-overleg, zaten er veel mensen aan tafel. Dit zorgde ervoor dat er gedisciplineerd overlegd moest worden om ruis te voorkomen. Hoewel dit geen optimale situatie is, blijkt dit niet tot knelpunten te hebben geleid in de crisisbeheersing.

E.2.6 Informatiemanagement

In het zorgcontinuïteitsplan is geen proces voor informatiemanagement opgenomen. De verantwoordelijkheid voor informatiemanagement is in het plan belegd bij het CBT. Uit de interviews met betrokken medewerkers is gebleken dat er in de praktijk ook geen structurele afspraken zijn gemaakt over de wijze waarop informatie wordt verzameld, gevalideerd, gepresenteerd, vastgelegd en gedeeld tijdens de crisisbeheersing. Ook het vastleggen van informatie en documenteren van besluiten door middel van gestandaardiseerde verslaglegging in CBT-overleggen is niet geregeld.

Dit heeft op 3 juni 2018 geen problemen opgeleverd, doordat de voorzitter CBT tijdens de CBT-overleggen van alle aanwezige artsen en de aanwezige ICT-medewerkers uit eerste hand heeft vernomen wat de stand van zaken was.

E.2.7 Crisiscommunicatie (intern)

In het strategisch kader van het zorgcontinuïteitsplan is beschreven dat de voorzitter van het CBT de interne en externe communicatie tijdens de crisis coördineert. Daarvoor maakt hij gebruik van de communicatiemedewerker die standaard aan het CBT is toegevoegd. In de beschrijving en in de praktijk blijkt de communicatieadviseur zich in lijn met het crisiscommunicatieplan voornamelijk te richten op de ondersteuning van de voorzitter CBT bij de externe communicatie. Er is bovendien geen procedure vastgesteld voor interne crisiscommunicatie en er zijn geen scenario's voorbereid voor de interne informatievoorziening als de reguliere communicatiemiddelen als gevolg van ICT-uitval niet beschikbaar zijn.

Doordat in de CBT-overleggen alle afdelingen waren vertegenwoordigd, vond de interne communicatie vooral daar plaats. Iedereen kreeg daar informatie over de stand van zaken en de acties die ondernomen dienden te worden. Tussentijds informeren bleek niet mogelijk, omdat de gebruikelijke interne communicatiemiddelen niet meer beschikbaar waren. Dit was niet eerder als een risico gezien en er waren dus geen alternatieven voorbereid. De CC heeft daarop geïmproviseerd en een WhatsApp-groep aangemaakt voor de deelnemers van de CBT-overleggen om de interne communicatie beter te kunnen ondersteunen.

26 BOBOC staat voor Beeldvorming-Oordeelsvorming-Besluitvorming-Opdracht-Controle.

E.2.8 Opleiden, trainen en oefenen

Aangewezen crisisfunctionarissen waren binnen het IJsselland Ziekenhuis opgeleid en getraind onder het ZiROP. In het zorgcontinuïteitsplan is de voorbereiding en training voor optreden tijdens crises en calamiteiten belegd bij het multidisciplinair veiligheidsteam. Het plan beschrijft doelen voor alle OTO-activiteiten voor de looptijd van het zorgcontinuïteitsplan, echter in het eerste loopjaar van het plan zijn er geen trainingen en opleidingen gehouden. Voor oefeningen is vanwege inhoud en uit kostenoverwegingen zoveel als mogelijk aangesloten op oefeningen van stakeholders. ICT-uitval is nooit eerder gebruikt als (onderdeel van) een scenario bij trainingen of als concreet oefendoel.

E.2.9 Evalueren

In het zorgcontinuïteitsplan is de verantwoordelijkheid voor het vastleggen van gebeurtenissen, beslissingen, getroffen maatregelen etc. ten behoeve van een evaluatie van de hulpverlening en een eventueel in te stellen onderzoek beschreven bij de algemene taken van het CBT.²⁷ De feitelijke verantwoordelijkheid voor het vastleggen van deze informatie is echter niet toegewezen aan een concrete functionaris binnen de crisisorganisatie. Op basis van de verslaglegging van de CBT-bijeenkomsten is geen goed beeld te vormen over de besluitvorming, de genomen maatregelen en de leerpunten van de ICT-storing van 3 juni 2018.

Het zorgcontinuïteitsplan heeft de verantwoordelijkheid voor het organiseren van een evaluatie niet concreet belegd, noch een proces daarvoor ingericht. Er heeft geen uitgebreide, systematische, evaluatie plaatsgevonden van de ICT-storing van 3 juni 2018. Ook bij eerdere voorvallen, zoals het perazijnzuurincident in het IJsselland Ziekenhuis, ontbrak een systematische evaluatie. Na afloop van de ICT-storing van 3 juni 2018 heeft wel een korte evaluatiebijeenkomst plaatsgevonden met de relevante deelnemers van het CBT. Omdat er van deze evaluatie geen verslag is gemaakt, is er geen beeld welke lessen getrokken zijn uit dit voorval.

Samenvattende conclusie

Het IJsselland Ziekenhuis heeft in 2018 de eerste stappen gezet om zich beter voor te bereiden op alle mogelijke in- en externe crises waar het ziekenhuis bij betrokken kan raken. Het onderzoek laat zien dat de hoofdlijnen van de crisisbeheersing op papier zijn uitgewerkt, maar dat de crisisorganisatie nog niet volledig is voorbereid op ICT-storingen. Op 3 juni 2018 ontbrak het namelijk aan (1) adequate handvatten voor dit type calamiteiten, (2) een proces voor informatiemanagement en (3) een plan voor de interne communicatie tijdens de crisis. Het ontbreken van goede vastlegging van gebeurtenissen, beslissingen en getroffen maatregelen tijdens de crisisbeheersing én het ontbreken van een uitgebreide, systematische, evaluatie staat het leren van dit incident in de weg.

²⁷ *Zorgcontinuïteitsplan, strategisch kader versie 6.0, mei 2018, pagina 12.*

E.3 Dijklander ziekenhuis

E.3.1 Visie en planvorming

Het Dijklander Ziekenhuis heeft de voorbereiding op mogelijke crisissituaties vastgelegd in het Integraal Crisisplan (ICP).²⁸ Het ICP brengt alle bestaande procedures, protocollen en plannen van de organisatie samen onder eenzelfde regime. In het bijzonder worden het bedrijfsnoodplan, het ZiROP en het crisiscommunicatieplan samengebracht. Het plan verbindt onderliggende plannen en beoogt daarmee bij te dragen aan een uniforme werk- en denkwijze, ongeacht het type crisis.

Het ICP is een uitwerking van de visie van het bestuur op het crisismanagement. Het beschrijft de werkwijze bij (dreigende) crisissituaties, zowel inhoudelijk als qua proces en organisatie. De verantwoordelijkheid voor de inhoud van het ICP ligt bij de stuurgroep Integraal Crisismanagement (ICM). De ICM wordt voorgezeten door de zorgmanager die crisisbeheersing in zijn portefeuille heeft en bestaat verder uit een lid van het medisch stafbestuur, de manager facilitair, de OTO-functionaris, het hoofd fysieke veiligheid, de beheerder ICP/ZiROP en secretariële ondersteuning. Het initiatief voor actualisatie van het ICP ligt bij de zorgmanager met crisisbeheersing in portefeuille. Het ICP wordt minimaal tweejaarlijks geactualiseerd door de beheerder, waarbij hij aan de hand van evaluaties, praktijkervaringen en/of trainingen/oefeningen naloopt of het plan nog toereikend is en zo nodig het plan bijstelt. Het plan dat ten tijde van het voorval van toepassing was, is vastgesteld in januari 2018.²⁹

E.3.2 Risicoanalyse

Het Dijklander Ziekenhuis gaat ervan uit dat crisissituaties kunnen ontstaan door situaties in de omgeving of de zorgketen waar zij deel van uitmaakt, dan wel door situaties in de eigen dienstverlening, organisatie of directe omgeving van de ziekenhuislocaties. Het Dijklander Ziekenhuis heeft, uitgaande van de eigen dienstverlening, de organisatie en de omgeving, acht externe risico's (waaronder uitval nutsvoorzieningen) en dertien interne risico's (waaronder uitval ICT) geïdentificeerd die kunnen uitgroeien tot een crisis. Deze risico's, waaronder ICT-uitval, zijn echter niet nader uitwerkt.

In het ICP is in een bijlage wel een scenariokaart *Cybercrisis* opgenomen, die handvatten geeft in geval het Dijklander Ziekenhuis 'in het hart getroffen wordt door een abnormale situatie waarbij strategische doelen, reputatie en betrouwbaarheid in het geding komen door een verstoring van de ICT, bewust of onbewust.'³⁰ Dit scenario kent ook elementen van uitval van ICT. Het scenario beschrijft dat een cybercrisis kan gaan om een storing, het onbedoeld/bedoeld beschikbaar/toegankelijk zijn van data of een moedwillige aanval en/of chantage. Verder wordt beschreven dat de bedrijfscontinuïteit moet worden gewaarborgd, de gevolgen voor de patiëntveiligheid moeten worden voorkomen en de onrust onder patiënten, medewerkers en derden moet worden beperkt. Er is echter nauwelijks uitgewerkt welke kritieke momenten voor de patiëntveiligheid er zijn en hoe

²⁸ *Integraal Crisisplan Westfriesgasthuis – Waterlandziekenhuis*, versie 4.0, januari 2018.

²⁹ *Integraal Crisisplan Westfriesgasthuis – Waterlandziekenhuis*, versie 4.0, januari 2018, pagina 2.

³⁰ *Integraal Crisisplan Westfriesgasthuis – Waterlandziekenhuis*, versie 4.0, januari 2018, pagina 19.

daar mee om moet worden gegaan. Het ontbreekt in de scenariokaart bovendien aan concrete risicobeheersmaatregelen.

E.3.3 Melden en alarmeren

In het ICP is een meldingsprocedure beschreven waarin is aangegeven dat degene die het incident constateert, handelt volgens de SAR-methode: (1) Signaleer, dat er iets mis is, (2) Alarmeer de beveiliging, (3) Reageer, neem de noodzakelijke maatregelen om het incident te bestrijden of te managen. Belangrijk daarbij is de centrale rol van de beveiliging. Die alarmeert crisisfunctionarissen om de eerste maatregelen te kunnen nemen en adviseert de melder wat deze kan doen of wat deze juist moet nalaten in die specifieke situatie. De beveiliging zal ook via de receptie de dienstdoende CC alarmeren. De CC informeert op basis van de eerste informatie en een in het ICP beschreven besluitboom³¹ waar nodig de voorzitter CBT.

Op 16 juli 2018 was het de CC zelf die een ICT-incident constateerde, doordat de ICT-voorzieningen die ze wilde gebruiken niet beschikbaar waren. Ze zocht direct contact met de manager ICT, waarop duidelijk werd dat er sprake was van een algehele uitval van ICT-voorzieningen en telefonie en dat kritische ICT-voorzieningen in het ziekenhuis niet meer functioneerden. Hierop heeft de CC volgens protocol³² opgeschaald naar het OCT en de RvB ingelicht.

De melding van de *failover*³³ van 14:12 uur had echter reeds moeten leiden tot alarmering van de crisisorganisatie. Immers vanaf dat moment was er sprake van een verhoogd risico op uitval van het ICT-systeem en daarmee voor de patiëntveiligheid. Er was vanaf dat moment sprake van een potentiële crisissituatie.

E.3.4 Op- en afschalen

De CC beoordeelt of er sprake is van een ernstige bedreiging voor de continuïteit en/of kwaliteit van de zorg. Dat is het geval als sprake is van twee of meer impactgebieden en/of als de mogelijkheid ontbreekt om het incident met de regulier beschikbare middelen op te lossen. Indien nodig zal de CC in eerste instantie een OCT instellen. Op basis van het in te schatten effect en impact van de crisis vindt dan verdere alarmering en opschaling tot en met het CBT plaats. In het ICP is een schema opgenomen dat handvatten geeft aan de CC voor besluitvorming over deze opschaling. Het gaat uit van vijf effectsituaties (minimaal, beperkt, substantieel, kritiek en catastrofaal).³⁴ Het ICP geeft geen beschrijving of handvatten hoe en wanneer de crisisorganisatie moet worden afgeschaald.

Op 16 juli 2018 is opgeschaald conform bovengenoemd proces. Bij het eerste OCT-overleg werd duidelijk dat op dat moment het gehele pand en alle zorgafdelingen werden geraakt door de ICT-storing en dat onduidelijk was hoe lang dit zou duren. Daarnaast was onduidelijk waarom het nood-EPD nog niet beschikbaar was. Op basis van deze onvoorspelbaarheid van de duur van het herstel werd besloten om de voorzitter

³¹ *Integraal Crisisplan Westfriesgasthuis – Waterlandziekenhuis, versie 4.0, januari 2018, pagina 9.*

³² *Integraal Crisisplan Westfriesgasthuis – Waterlandziekenhuis, versie 4.0, januari 2018.*

³³ Hiermee wordt de overschakeling van de primaire naar de secundaire mode bedoeld.

³⁴ *Integraal Crisisplan Westfriesgasthuis – Waterlandziekenhuis, versie 4.0, januari 2018, pagina 10.*

van de RvB te adviseren tot een opnamestop op de SEH en werd volgens protocol opgeschaald naar het CBT. Het dienstdoende lid van de RvB werd door de CC ingelicht over de voorgenomen sluiting van de SEH. Besloten werd om binnen vijftien minuten een gecombineerde OCT/CBT-overleg bijeen te roepen, waar uiteindelijk alle kritische afdelingen vertegenwoordigd waren.

E.3.5 Leiding en coördinatie

Het Dijklander Ziekenhuis heeft de taken en de verantwoordelijkheden van de functionarissen binnen de crisisorganisatie uitgewerkt in het ICP en de bijbehorende taakbladen. De voorzitter van de RvB is eindverantwoordelijk voor de crisisbeheersing en de CC is verantwoordelijk voor het in werking stellen van de crisisorganisatie. In het scenario *Cybercrisis* is onder de kop 'bijzonderheden in de voorbereiding' aangetekend dat de aansluiting van de ICT-organisatie op de crisismanagementstructuur een risico kan zijn. Dit is binnen het kader van dit scenario echter niet nader uitgewerkt in passende risicobeheersmaatregelen.

De leiding en coördinatie heeft tijdens het voorval op 16 juli 2018 conform de in het ICP beschreven taken en verantwoordelijkheden plaatsgevonden. Er was gedurende het incident echter onvoldoende zicht op de voortgang van de technische incidentbestrijding bij de afdeling ICT. Dat kan voor een deel verklaard worden doordat de opschaling van de ICT-organisatie niet aansloot op de in het ICP beschreven opschaling. Dit was een risico dat was voorzien in het scenario *Cybercrisis*.

E.3.6 Informatiemanagement

Het Dijklander Ziekenhuis heeft geen uitgewerkt proces voor informatiemanagement in de crisisorganisatie. Het ziekenhuis heeft aangegeven dat de CC in de praktijk de rol van informatiecoördinator vervult. Bij crisissituaties met grote impact wordt er een extra CC in dienst geroepen die de functie van informatiecoördinator vervult. Het Dijklander Ziekenhuis is op zoek naar een informatiemanagementsysteem wat hiervoor gebruikt kan worden. Echter, vanwege het fusieproces van het Dijklander Ziekenhuis is het opzetten van een goed informatiemanagementproces voor de crisisorganisatie nog niet opgestart. De fusie krijgt, vanwege de noodzakelijke voortgang in de integratie van bestaande processen, prioriteit boven de invoering van nieuwe zaken zoals een informatiemanagementsysteem.

Informatiemanagement heeft een rol gespeeld bij de ICT-storing van 16 juli 2018. Het eerder genoemde beperkte zicht van de crisisorganisatie op de voortgang bij de technische incidentbestrijding bij de afdeling ICT, werd niet alleen veroorzaakt door de onvolkomenheden in de leiding en coördinatie (zie hierboven), maar ook door het ontbreken van een uitgewerkt proces voor informatiemanagement. Dit werd in de hand gewerkt door onvoldoende eenduidige beeldvorming binnen het OCT. Dit werd mede veroorzaakt door het feit dat binnen de ICT-organisatie ook wisselende signalen bestonden over de voortgang. Het crisisteam had lange tijd het beeld dat de incidentbestrijding zowel werkte aan het herstel van het systeem als aan de reparatie van

de defecte *controller*³⁵, terwijl de incidentbestrijding zich lange tijd eenzijdig op systeemherstel had gericht. De problemen in de voortgang van de reparatiewerkzaamheden waren niet in beeld en kwamen ook onvoldoende naar voren in de terugkoppeling binnen het OCT. Hierdoor heeft de crisisbestrijding later dan mogelijk geëscaleerd om de reparatie van de *controller* te bewerkstelligen.

E.3.7 Crisiscommunicatie (intern)

Het Dijklander Ziekenhuis heeft in het ICP geen specifiek proces voor interne crisiscommunicatie beschreven. De voorzitter van het CBT is verantwoordelijk voor communicatie en perswoordvoering. Als er alleen een OCT is opgeschaald, is de voorzitter van het OCT verantwoordelijk voor de interne crisiscommunicatie. Afhankelijk van de mate van opschaling (OCT of CBT) beschikt de betreffende voorzitter over een communicatieadviseur die inhoudelijk verantwoordelijk is voor de interne communicatie. Het ICP bevat een checklist crisiscommunicatie³⁶ die concrete vragen, uitgangspunten en strategieën beschrijft als hulpmiddel voor de communicatieadviseur en medewerkers communicatie voor crisiscommunicatie. In het scenario *Cybercrisis* is aangetekend dat als ICT-systemen zijn aangetast of moeten worden uitgezet, dit kan leiden tot mogelijke kwetsbaarheden in de communicatie. Dit is binnen het kader van dit scenario niet nader uitgewerkt in passende risicobeheersmaatregelen.

Door de ICT-uitval op 16 juli 2018 ontbraken de gebruikelijke interne communicatiemiddelen om alle medewerkers op de hoogte te houden van de voortgang van de crisis en de geldende beheersmaatregelen. Hoewel dit in het scenario *Cybercrisis* was voorzien, waren er geen uitgewerkte alternatieve communicatiemiddelen voorbereid. Medewerkers waren daardoor gedurende het verloop van het voorval niet allemaal geïnformeerd over de geldende beheersmaatregelen. Zo was de communicatie over het regime van beperkt gebruik van de ICT-voorzieningen niet altijd eenduidig, wat zorgde voor onrust en onduidelijkheid.

E.3.8 Opleiden, trainen en oefenen

De stuurgroep ICM draagt zorg voor de geoefendheid van alle bij de crisisbeheersing betrokken functionarissen. De stuurgroep heeft geen specifiek OTO-plan vastgesteld voor het ICP, maar crisisfunctionarissen zijn wel opgeleid en getraind³⁷ conform het OTO-jaarplan ZiROP. Hoewel de samenstelling van het OCT in de ZiROP-opschaling anders is ingeregeld³⁸, zijn de taken en verantwoordelijkheden van de meeste functionarissen vergelijkbaar. Echter, vanwege de inhoudelijke verschillen in begrippen, procedures en verantwoordelijkheden, brengt het ontbreken van op het ICP afgestemde OTO-training het risico met zich mee dat functionarissen onvoldoende zijn voorbereid op hun rol. In de aangeboden OTO-activiteiten is ICT-uitval niet gebruikt als (onderdeel van) een scenario.

³⁵ Een controller is een element in een storagestelsel dat de functie heeft om data weg te schrijven en op te halen van de opslagdisks van de storage.

³⁶ *Integraal Crisisplan Westfriesgasthuis – Waterlandziekenhuis, versie 4.0*, januari 2018, bijlage D *Checklist crisiscommunicatie*, pagina 18.

³⁷ *Retrospectieve analyse ICT - storing 16-17 juli 2018*, 25 oktober 2018, pagina 24.

³⁸ In de ZiROP werkwijze wordt het ziekenhuis in 6 compartimenten opgedeeld met bijbehorende compartimentscoördinator, in de ICP werkwijze wordt de crisisbeheersing centraal aangestuurd met één crisiscoördinator: *Integraal crisisplan Westfriesgasthuis versie 4.0*, januari 2018, pagina 10.

E.3.9 Evalueren

In het ICP is vastgelegd dat er enige tijd na de crisis een goede en zorgvuldige evaluatie moet plaatsvinden. De CC, die tijdens het incident dienst heeft gehad, moet het initiatief nemen om het proces en het verloop van de crisis te evalueren. Zowel met alle personen die een rol hadden in het OCT of het CBT als met de medisch managers en de leidinggevenden van de afdelingen die bij de crisis of de afhandeling van de crisis betrokken waren. De CC zet daartoe, via de *risk officer* (of bij diens afwezigheid de secretaris van de RvB), vragenlijsten uit bij de personen die het aangaat. De *risk officer* maakt een analyse van de ingevulde vragenlijsten. De secretaris van de RvB maakt op basis van deze analyse een eindverslag voor bespreking in de RvB en als input voor bespreking in de stuurgroep ICM om het ICP en de daaruit voortvloeiende planvorming en OTO-activiteiten voor toekomstige crises te verbeteren.

De ICT-storing van 16 juli 2018 is in lijn met dit proces geëvalueerd en verwerkt tot een rapportage waarin leermomenten voor de organisatie zijn benoemd en als aanbevelingen aan de stuurgroep ICM en de RvB zijn aangeboden.³⁹ De vragenlijst is door 32 deelnemers uit de crisisorganisatie ingevuld en er zijn twaalf nadere gesprekken met medewerkers gevoerd om een duidelijker beeld te krijgen van de mogelijk leermomenten en verbeterpunten. Daarnaast is er een afzonderlijke evaluatie geweest van de Prospectieve Risico Analyse, die de start vormde van de werkzaamheden die aan de basis lagen van de ICT-uitval. Hierbij waren vertegenwoordigers van de afdeling ICT, facilitair bedrijf en het externe bedrijf betrokken.

De Onderzoeksraad constateert dat in de evaluatie beperkt aandacht is besteed aan de gevolgen voor (de veiligheid van) de patiënten in het ziekenhuis. Zo wordt in de eindevaluatie wel ingegaan op de patiëntveiligheid tijdens de crisissituatie, maar ontbreekt een diepgaande analyse van de afhankelijkheden van de zorgprocessen van ICT en de gevolgen daarvan voor de patiëntveiligheid bij deze ICT-uitval.⁴⁰ Met betrekking tot de onderzochte ICT-storing geven diverse betrokkenen aan dat er geen schade is geweest voor patiënten, maar een analyse op patiënt- en/of afdelingsniveau ontbreekt. Er is bovendien beperkt zicht op patiënten die zijn omgeleid doordat ze niet bij het Dijklander Ziekenhuis terecht konden tijdens de ICT-storing.

³⁹ Retrospectieve analyse ICT-storing 16-17 juli 2018, 25 oktober 2018.

⁴⁰ Retrospectieve analyse ICT-storing 16-17 juli 2018, 25 oktober 2018.

Samenvattende conclusie

Het Dijklander Ziekenhuis heeft in 2018 alle bestaande procedures, protocollen en plannen voor de voorbereiding op alle mogelijke crisissituaties samengebracht in een nieuw ICP. Daarbij ontbreekt een uitwerking in deelplannen voor belangrijke risico's, zoals ICT-uitval. Een belangrijk probleem tijdens de crisisbeheersing was dat bij de crisisorganisatie lange tijd onvoldoende duidelijk was dat er problemen waren in de voortgang van de reparatiewerkzaamheden. Dit werd enerzijds veroorzaakt doordat de opschaling van de ICT-organisatie niet goed aansloot bij de opschaling van de crisisorganisatie én anderzijds doordat het informatiemanagement niet goed was vormgegeven. Bij de evaluaties van ICT-incidenten in het Dijklander Ziekenhuis, ten slotte, wordt in beperkte mate aandacht besteed aan de gevolgen voor de veiligheid van de patiënten in het ziekenhuis.