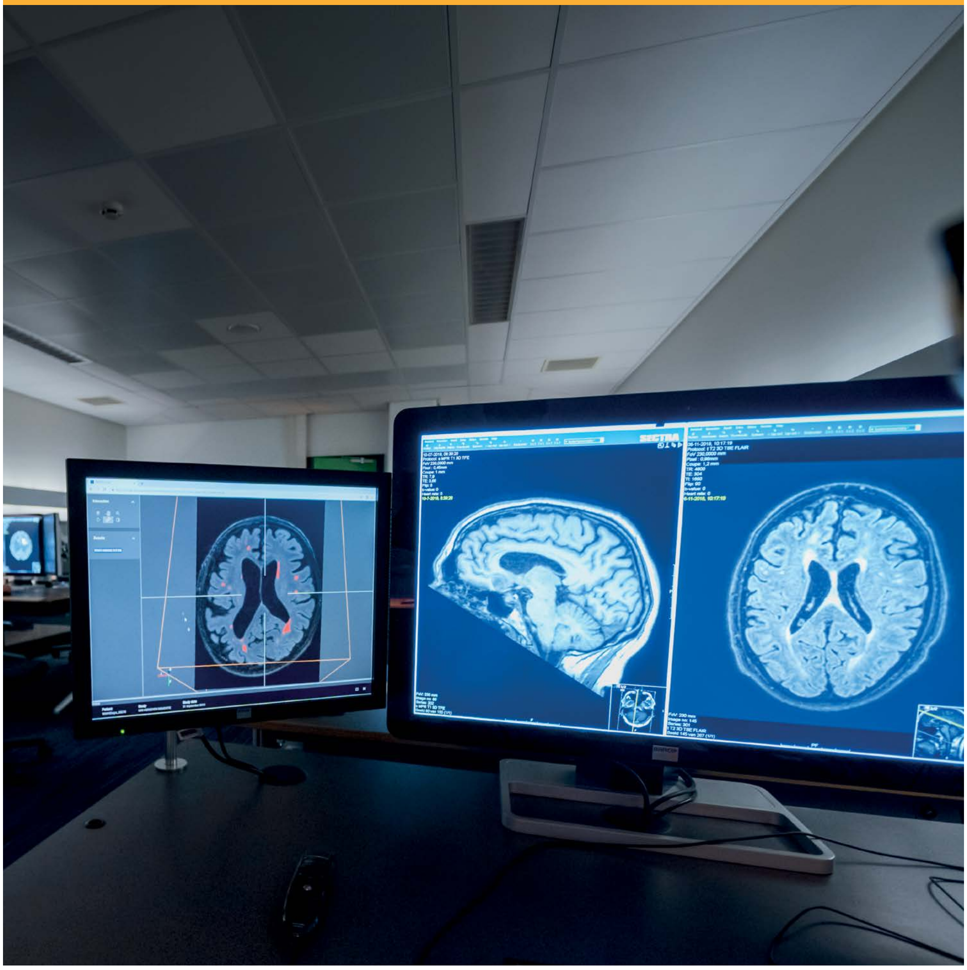
DUTCH
SAFETY BOARD

Patient safety during IT outages in hospitals



Patient safety during IT outages in hospitals

The Hague, February 2020

Image cover: mr. O. Middendorp

The Dutch Safety Board

When accidents or disasters happen, the Dutch Safety Board investigates how it was possible for these to occur, with the aim of learning lessons for the future and, ultimately, improving safety in the Netherlands. The Safety Board is independent and is free to decide which incidents to investigate. In particular, it focuses on situations in which people's personal safety is dependent on third parties, such as the government or companies. In certain cases the Board is under an obligation to carry out an investigation. Its investigations do not address issues of blame or liability.

	Dutch Safety Board		
Chairman:	J.R.V.A. Dijsselbloem M.B.A. van Asselt S. Zouridis		
Secretary Director:	C.A.J.F. Verheij		
Visiting address:	Lange Voorhout 9 2514 EA The Hague The Netherlands	Postal address:	PO Box 95404 2509 CK The Hague The Netherlands
Telephone:	+31 (0)70 333 7000		
Website:	safetyboard.nl		
E-mail:	info@safetyboard.nl		

N.B. The full report is published in the Dutch language. If there is a difference in interpretation between the Dutch report and English summary, the Dutch text wil prevail.

CONTENT

CONSIDERATIONS

In recent decades, critical social services and processes have become increasingly dependent on the uninterrupted availability of digital systems. The drinking water supply, water management, and emergency services' communication systems all depend on digital systems. This also applies to hospitals, where IT systems have penetrated to the heart of the healthcare process. Many hospital processes, such as accessing patient data, making appointments, sharing laboratory results and dispensing drugs, can only be carried out if the IT systems are functioning. As such, hospitals have become IT companies in their own right. Moreover, this dependency on IT will only increase in the future. For example, it is expected that critical equipment on and around hospital beds will become increasingly dependent on the hospital IT network, and that remote monitoring of patients via phones or tablets will become daily practice. Analogue work processes are being phased out at a steady pace, so that it is no longer possible to fall back on these if an IT system fails.

The far-reaching digitization of healthcare in hospitals offers opportunities to improve this care, but at the same time brings new risks. IT failures are such a risk; one defective component or the wrong network setting can shut down the primary healthcare processes in a hospital for hours or even days. This has implications for the quality and safety of patient care. Although the incidents investigated by the Dutch Safety Board to date are not known to have involved any injury to patients, it is clear that there is an increased risk of this happening.

During its investigation of these incidents, the Dutch Safety Board observed that the hospitals primarily measured the consequences for patient safety in terms of the actual damage caused to the patients. The increased risk of damage caused by the incidents was largely disregarded and was often not evaluated. Moreover, the evaluations paid too little attention to the consequences of the IT outages for the safety of inpatients and for patients who had to be diverted to another hospital because of the disruption. The obvious conclusion is that hospitals have only limited insight into the risks of IT failures for their patients. This insight into these risks for patient safety is an important prerequisite for adequate risk management.

The number of major computer system failures that have occurred in the Netherlands in recent years is ample proof that hospitals need to take the risk of IT disruptions seriously. Although no central registration takes place, news reports reveal that at least ten hospital organizations were affected by a major IT outage in 2019. This is considerably more than five years ago, in 2015, when only one major IT disruption was reported in the media. Moreover, due to the changing healthcare landscape, IT outage increasingly result in a loss of healthcare capacity affecting several locations in a wider area. For example, a total of 28 healthcare locations were affected by the ten large-scale IT outages reported in 2019.

This IT dependency is not unique to the hospital sector; other sectors are affected too. A good example is the financial sector, which is considered to play a 'vital' role in the Netherlands[1]. The Netherlands is one of the frontrunners in digital payments in Europe. Digital payments are fast and easy for customers and safe and efficient for retailers. In the event of failure of a PIN device, however, a large proportion of payment traffic will come to a standstill, because many customers do not have cash with them or because shopkeepers only accept PIN payments. Banks have taken measures in recent years to prevent payment system failures (and the related social disruption) and to ensure IT systems are made operational again as soon as possible following a failure.

The continuity of healthcare provision is critical for the welfare of the Dutch population. A number of years ago, the Ministry of Health, Welfare and Sport decided not to designate hospitals and other healthcare providers as 'vital'. The Network and Information Systems Security Act[2], introduced in 2018, therefore does not apply to hospitals. This decision is currently being reconsidered, which may result in hospitals (or specific hospital processes or units) having to comply with the requirements of that act in 2020. It is up to the Minister of Health and Sports to decide whether the findings and conclusions in this report give cause to revise the decision and designate hospitals as 'vital'.

In any case, the increasing dependence on IT obliges the hospital sector to put its digital resilience in order. The current report offers a number of starting points to help the sector achieve this. It goes without saying that hospitals will need focus on the prevention of IT outages, for example by improving the design and management of their IT systems, however that will not be enough. Due to the complexity of IT systems, some of the risks are unpredictable, which means that failures cannot always be prevented. But measures can be taken to mitigate the consequences of an IT failure as much as possible. This means that hospitals need to prepare for every eventuality and ensure that hospital staff can respond adequately. For example, hospital emergency response teams need to be better equipped to deal with the specific characteristics of IT failures, both by preparing detailed emergency response plans and through training and exercise. Dependencies between healthcare and IT must also be identified to be able to predict how IT failures could affect the quality and safety of patient care. The systems that prove to be the most critical must be made redundant as much as is reasonably possible. To this end, it is important to test IT systems (and combinations of systems) periodically to ensure that critical healthcare processes can continue to function under all circumstances.

The number of IT failures in recent years suggests that this problem has existed for longer and is not limited to the three hospitals investigated. The Dutch Safety Board believes that hospitals must identify in what ways their dependence on IT poses risks for patients.

[1] Processes such as payments have been identified as 'vital' for the financial sector. A total or partial failure of these processes can have major social and/or financial and economic consequences. A process is 'vital' if a failure would lead to:
- more than €5 billion of damage or a 1.0% reduction in real income
- more than 1,000 fatalities, seriously injured or chronically ill victims
- more than 100,000 people experience emotional problems or severe social problems.

[2] Network and Information Systems Security Act, formerly also referred to as the Cyber Security Act. This act implements the European NIS Directive. The purpose of this Directive is to bring unity and coherence to European NIS policies by increasing digital preparedness and reducing the impact of cyber incidents, all with the aim of helping society and the economy to function.

IT failures have grown into a risk that deserves the same attention that hospitals pay to more traditional risks (such as inadequate hand hygiene). This issue is not only the responsibility of the hospital's IT departments, but also needs to have a place in medical staff meetings and in the boardroom.

RECOMMENDATIONS

The healthcare provided in hospitals is increasingly dependent on the proper functioning of hospital IT systems. This investigation has revealed how IT failures can jeopardize patient safety. The Dutch Safety Board has identified starting points for hospitals to identify the risks of IT outages at an early stage and effectively manage the consequences of these outages for patient safety. On the one hand, they need to focus more on the prevention of computer system failures, while on the other they need to improve their response to the consequences of an IT failure.

The frequency and duration of known IT failures in hospitals reveals that this is a widespread issue. The Dutch Safety Board has therefore decided not to limit its recommendations to the three hospitals investigated, but to address all hospitals in the Netherlands. To encourage hospitals to approach the issue as a sector, and learn from and with each other to adequately manage the risks of IT outages, the Dutch Safety Board has decided to direct its recommendations at the two largest sector associations. The Dutch Safety Board also sees a role for the Health and Youth Care Inspectorate (IGJ) in this.

To the Dutch Association of Hospitals (NVZ) and the Dutch Federation of University Medical Centres (NFU):

1. Ensure that your members:

    a. Periodically identify the dependencies between healthcare and IT, including the possible risks for patients associated with IT failures, to ensure adequate preparedness for IT failures.
    b. Periodically test IT systems (and combinations of systems) to ensure that critical healthcare processes can continue to function under all circumstances. Also conduct training exercises for emergency scenarios whereby the hospital's IT systems fail. Involve the suppliers of the systems in these exercises and tests where appropriate.
    c. Conduct evaluations after every serious IT failure in which the damage (and increased risk of damage) to both patients in the hospital and diverted patients is analysed in depth. Involve the partners in the healthcare chain where necessary.
    d. Publicly demonstrate their accountability for all three of these aspects on an annual basis.

2. Ensure that hospitals approach the issue as a sector and learn from and with each other.

3. Develop a practical tool for hospitals to manage the risks of IT outages, taking into account the starting points mentioned in this report.

4. Ascertain whether the safety of patients is sufficiently guaranteed in the event of an IT outage that affects several hospital locations in a region.

To the Health and Youth Care Inspectorate (IGJ):

5. Integrate the starting points in the above recommendations in the regulatory supervision of hospitals.

CONCLUSIONS

The Dutch Safety Board investigated how hospitals can adequately manage the risks of IT failures to patient safety. To this end, the Board evaluated three computer system failures in hospitals. The investigation has resulted in the following primary conclusion:

Digitization has penetrated to the heart of the healthcare sector. Virtually all processes in hospitals have been digitized to a greater or lesser extent. As a result, the provision of adequate diagnoses and treatment have become virtually impossible without digital techniques. Hospitals have hence become increasingly dependent on the proper functioning of their IT systems to provide adequate and safe healthcare and this means that major IT failures can have a direct impact on patient safety. The Dutch Safety Board observes that, while hospitals are becoming increasingly dependent on IT systems, their awareness of the risks of IT failures has not kept pace with this dependency. In order to improve their management of the risks to patients, hospitals need to pay more attention to the prevention of IT failures, the resolution of these failures, and mitigating the consequences of IT failures for patient safety.

This primary conclusion is based on four secondary conclusions:

1. *IT dependency of healthcare processes*

As a result of digitization, (specialist) healthcare provided in hospitals has become so dependent on IT that major computer system failures can result in unsafe situations for patients. To ensure the adequate and safe treatment of patients, hospitals need to identify the dependencies between healthcare and other processes and their IT systems.

2. *Preventing and resolving IT failures and managing their consequences*

Preventing IT failures depends on properly designed and managed IT systems. To be able to prevent IT failures, resolve them as quickly as possible if they do occur, and manage their consequences, hospitals need to be adequately prepared for IT failures and learn from the response to them. In the incidents investigated by the Board, hospital IT systems were down for long periods of time due, among others, to inadequate choices taken when establishing and managing the systems, and preparing the response to failures.

3. *Consequences of IT failures for patient safety*

The Dutch Safety Board has identified seven scenarios in which IT outages can cause damage to patients or increase the risk hereof. In order to learn from incidents and adequately manage the risks of IT failures, it is important that hospitals have as much as possible insight into the consequences of IT failures for patient safety. During the IT failures investigated, the healthcare professionals and managers always put patient safety first.

However, *after* the failures had been resolved, there was little systematic evaluation of their consequences – if any. When asked whether patient safety was at stake during the IT failure, the hospitals based their answer primarily on their evaluations of the actual damage that occurred, and paid very little attention – if any – to the occurrence of unsafe situations for the patients. Moreover, the evaluations paid too little attention – if any – to the consequences of the computer system failures for the safety of the inpatients. Finally, neither the hospitals that were investigated nor other parties in the sector have a clear picture of the possible damage that was caused by patients having to be diverted to another hospital.

4. Importance of attention for IT failures at the board level

An essential condition for the adequate management of IT failure risks and their consequences for patient safety is that this issue is taken up at the board level. Particular attention should be paid to the points made in the last three secondary conclusions above. It is also important that hospital staff have a shared sense of risk. Furthermore, the worlds of healthcare and IT need to be brought closer together so that the risks of IT failures and the potential consequences of these for adequate and safe healthcare can be recognized in good time.

DUTCH
SAFETY BOARD

Visiting address
Lange Voorhout 9
2514 EA The Hague
T 070 333 70 00
F 070 333 70 77

Postal address
PO Box 95404
2509 CK The Hague

www.safetyboard.nl