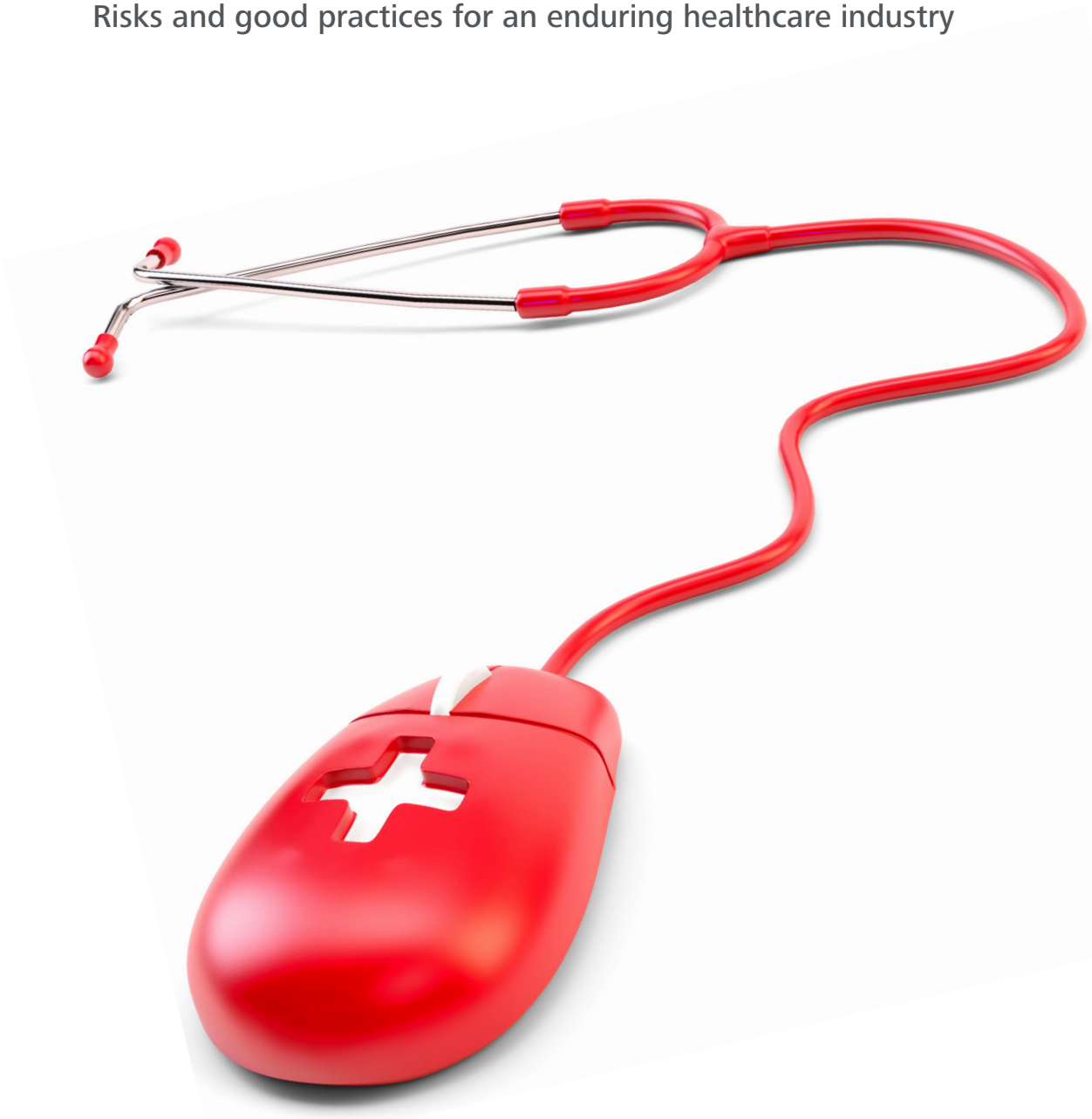
Deloitte.

Cybersecurity of network-connected medical devices in the Netherlands 2015

Risks and good practices for an enduring healthcare industry



Ir. Jeroen Slobbe
Tel: +31 88 288 27 53
E-mail: jslobbe@deloitte.nl

Contents

Introduction

Ever since the US "Government Accountability Office" (GAO) published its report on the hacking of medical devices, this topic has enjoyed more attention. As most of this report relates to US research, Deloitte has initiated research into the security status of medical devices in the Netherlands.

Between late 2013 and early 2015 we conducted interviews on the cybersecurity of medical devices at 17 of the 82 Dutch hospitals. We interviewed Heads of Medical Technology, Heads of IT, (Chief) Information Security Officers, Privacy Officers, medical specialists, and doctors.

A broadly observed trend is the ever growing number of network-connected medical devices. This encompasses machines like heart monitors, infusion devices, and MRI scanners. The increased connectivity creates threat scenarios and they may immediately affect patient safety. Examples are:

- Patients in need of therapy are cut off from such therapy because a signal on a device is blocked;
- Patients are given therapy without needing it, because a hacker has ordered such therapy;
- Patients are given therapy through a device in which a hacker has changed the settings. The patients now receive a different therapy than what they actually need;
- An alarm goes off where it should not go off, because a hacker has ordered this alarm to go off. This may cause alarm fatigue while at the same time nurses may temporarily be unable to respond to real alarms;
- An alarm fails to go off because a hacker actively blocks this, while the alarm should actually go off (availability).

This report discusses the results of the interviews. We likewise present the lessons learned and the good practices we have identified over the last year. We hope to provide you with new insights and for you to join us in taking follow-up steps to protect medical devices against cyber threats.

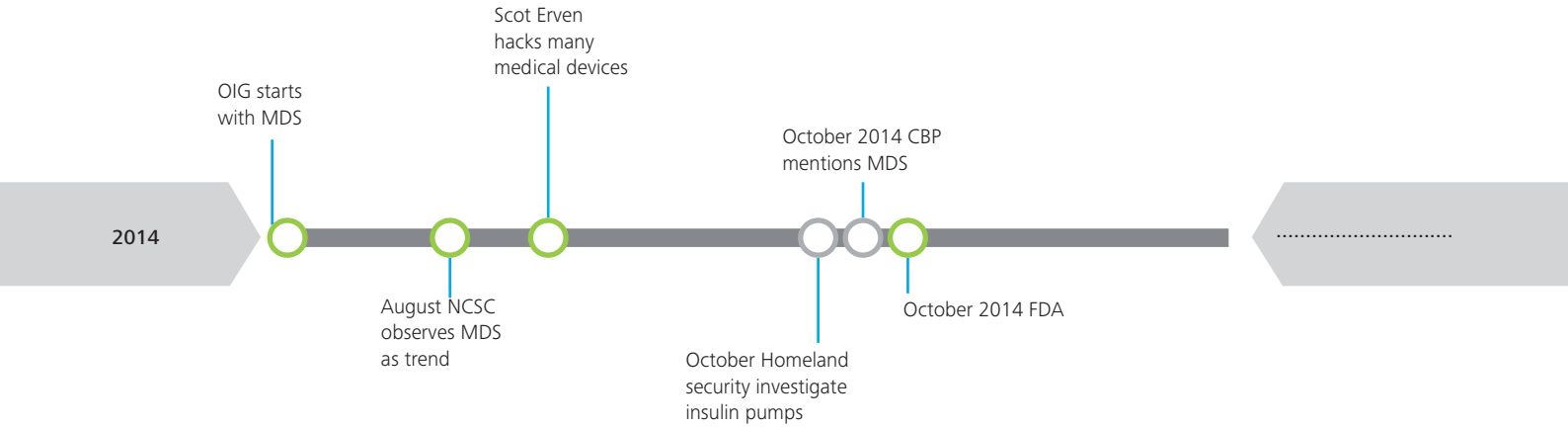
Approach

Under the promise of strict anonymity, we interviewed 17 different Dutch hospitals. These hospitals are different in size, location and type (general/academic). Over a period of 1.5 years we talked to several hospital professionals who often work with medical devices and/or IT. Before starting the actual interviews we gave a presentation about the risks described in literature and the research conducted in America. This was followed by an interview with the hospital staff.

The Deloitte team subsequently reviewed the minutes to make sure the answers had been properly transcribed to paper, after which they could be processed in the statistics.

2014 events involving the security of medical devices

While many devices were hacked in 2013, government agencies started to home in on Medical Device Security in 2014. Agencies like the Office Inspector General (the US healthcare inspectorate), Homeland Security, the FBI, and the FDA – they all pounced on this new technology and the associated risks. The Dutch National Cyber Security Center's cybersecurity policy flagged cybersecurity of medical devices as a threat. The Dutch Data Protection Authority, too, issued a statement about the necessity of network-connected medical devices having adequate security in place. And Hollywood was eager to jump the bandwagon by creating scenarios in series like "Homeland" and "Person of interest", in which people were hacked and damaged.



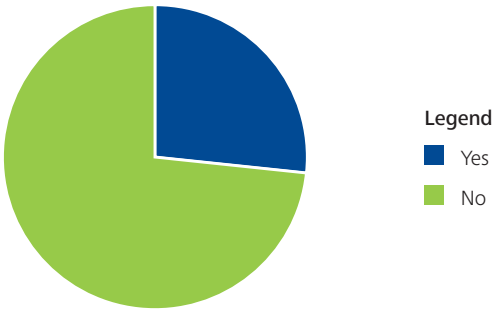
Results interviews

All hospital staff interviewed identified a clearly rising trend of medical equipment being connected to a network. The other questions have not been answered unanimously. We will address them below.

Policy, physical security and the removal of medical equipment

Policy

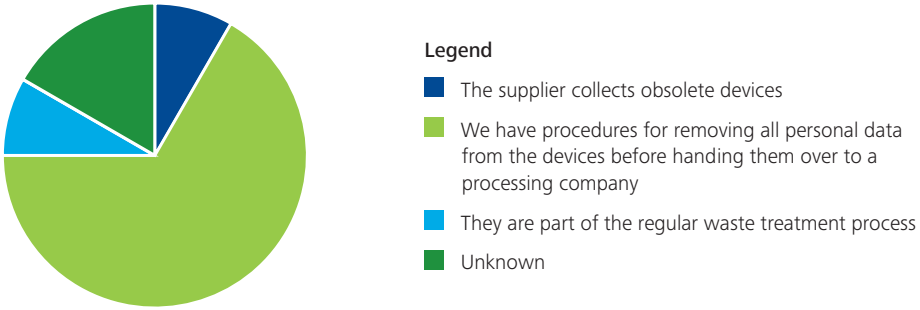
Four out of all hospitals interviewed stated to have an explicit information security policy in place for medical devices. The other thirteen hospitals stated to have no such policy



Having a clear policy for the cybersecurity of medical devices is important. We found Medical Technology and IT to sometimes be two entirely different departments. As a result, the responsibilities as regards cybersecurity of medical devices were not clear. A sound policy can clarify this.

Privacy during removal

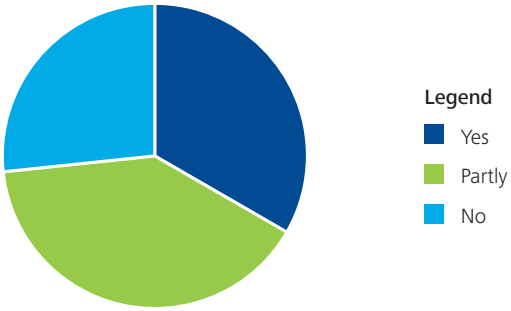
Eight of the hospitals interviewed stated to have a procedure for the removal of medical devices (if obsolete or no longer working). In one case most devices are collected by the supplier and in another case the devices are handed over to a professional waste treatment company. In two cases the devices are destroyed by a certified party. Hospitals without an internal data destruction procedure assume the suppliers and certified processors themselves to remove the data in an adequate manner. This question was missing from our standard questionnaire. We added this question to the set of questions later on, so the statement on this subtopic is less significant than on the other subtopics.



The risk of not removing data from medical devices, or not removing them adequately enough, is that privacy-sensitive information may unacceptably end up in the wrong place.

Physical security

Seven of the hospitals interviewed stated to keep larger medical devices in a locked room, while this partly applies to six hospitals. In four cases all hospital staff has access to the rooms where medical devices are located.

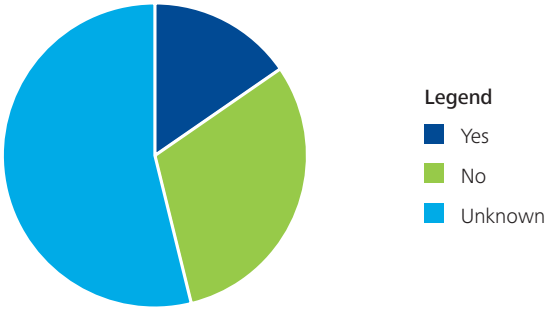


In some cases it is logical for medical devices to be accessible to everyone in the hospital. One such example is a hart monitoring device linked to a patient who has permission to receive visitors. Still, patients, visitors, and others should be prevented from plugging in unauthorized devices (such as smartphones and USB sticks). Implementing physical access security for MRI scanners could be one of the options.

Data protection

Communication encryption

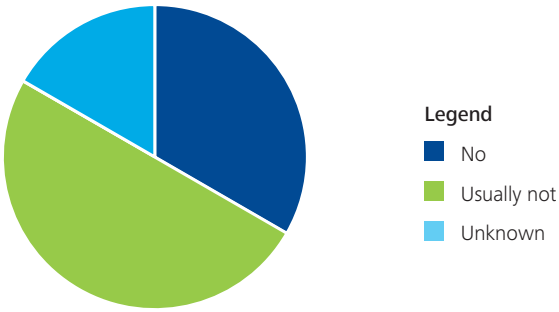
Two of the hospitals interviewed indicated their medical devices generally communicate over the network using an encrypted connection. Six hospitals stated this was generally not the case, while seven hospitals stated this was unclear to them.



Separate risks exist for separate network architecture frameworks and various options are available to mitigate such risks in the event of a lack of communication. This may be done by, e.g., implementing network segregation or network access controls. Not implementing such measures may create the risk of network traffic on a non encrypted network of medical devices. As a result, data confidentiality cannot be safeguarded. What's more (provided no additional measures have been taken), the integrity of the information sent may be compromised. This may ultimately result in a patient security risk or a breach of patient privacy.

USB stick encryption

Eight of the hospitals interviewed stated it was usually not possible to encrypt data on USB sticks. Four hospitals stated this is not possible at all within their organizations



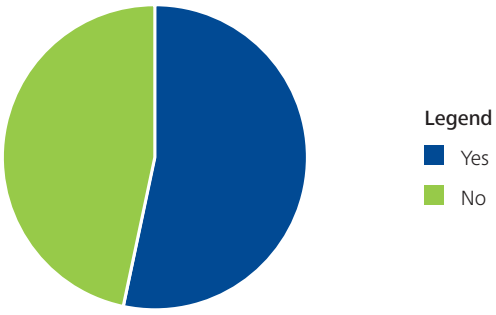
There is a risk of unencrypted sensitive data ending up on USB sticks, which increases the risk of data leakage. Another issue is the difficulty of safeguarding data integrity if this is transferred to the medical system once again from USB sticks.

Hospitals may consider sealing USB connections (if possible). If a connection is necessary for the system to function or to enable communication with other devices, a separate system may be put in place through which USB sticks are first checked for viruses before being used.

A secure solution for providing patients with images or data is to offer these data on a new USB stick, supplied by the hospital itself.

Computer viruses

Ten of the hospitals interviewed stated to have found computer virusses on their medical devices.



Computer viruses are a major risk. The integrity and operation of medical devices can no longer be guaranteed if they have been affected by a computer virus. Some viruses may cause performance problems. This will endanger the availability of the devices. A hospital's operational processes - and on the back of this its treatments - may be jeopardized if they depend on such devices.

Installing virus scanners on medical devices is not always the solution: not all equipment supports this, while hospitals do not always have the authorization to install software on devices they have procured. In addition to network segmentation, systems like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) may offer a solution. They allow devices to be used in the same way as they are currently used but offer better protection against malware infections.

Good practices and tips

When we conducted the interviews we came across a number of good practices: policy, network segregation, a single person responsible for ICT and Medical Technology (MT), Awareness, and listing the devices including the related risk assessments. The following figure presents the good practices identified.

A single person responsible for ICT and MT

A single person responsible for ICT ensures quicker switching between ICT and MT. What's more, the tasks and responsibilities will be clearly defined.

Network segregation

The administrative network should be separated from the medical network if the risk is to be mitigated. Likewise, devices can be subdivided into network groups as an additional layer of internal security against mass infections.

Policy

Having a data security policy for medical devices will clearly define the tasks and responsibilities. It should likewise guarantee the collection of the correct information during the procurement process.

Awareness

As more medical technicians and IT people are up-to-date about the cyber risks of network-connected medical devices, potential threats will be identified a lot quicker and adequate action will be follow.

Listing devices, connectivity and risks

Having an up-to-date and complete list of network-connected medical devices, including their features and cyber risk profiles, is important.

Conclusion

When we started this research we found out this was a new issue for hospitals. As we went on to conduct the interviews we noticed more and more professionals who were up to speed about the latest developments in the security of medical devices.

As yet, not using medical devices represents a larger risk to patients' health right now than using vulnerable medical devices. Vulnerabilities can be mitigated quite easily in some cases, though. It is recommended to start doing so.

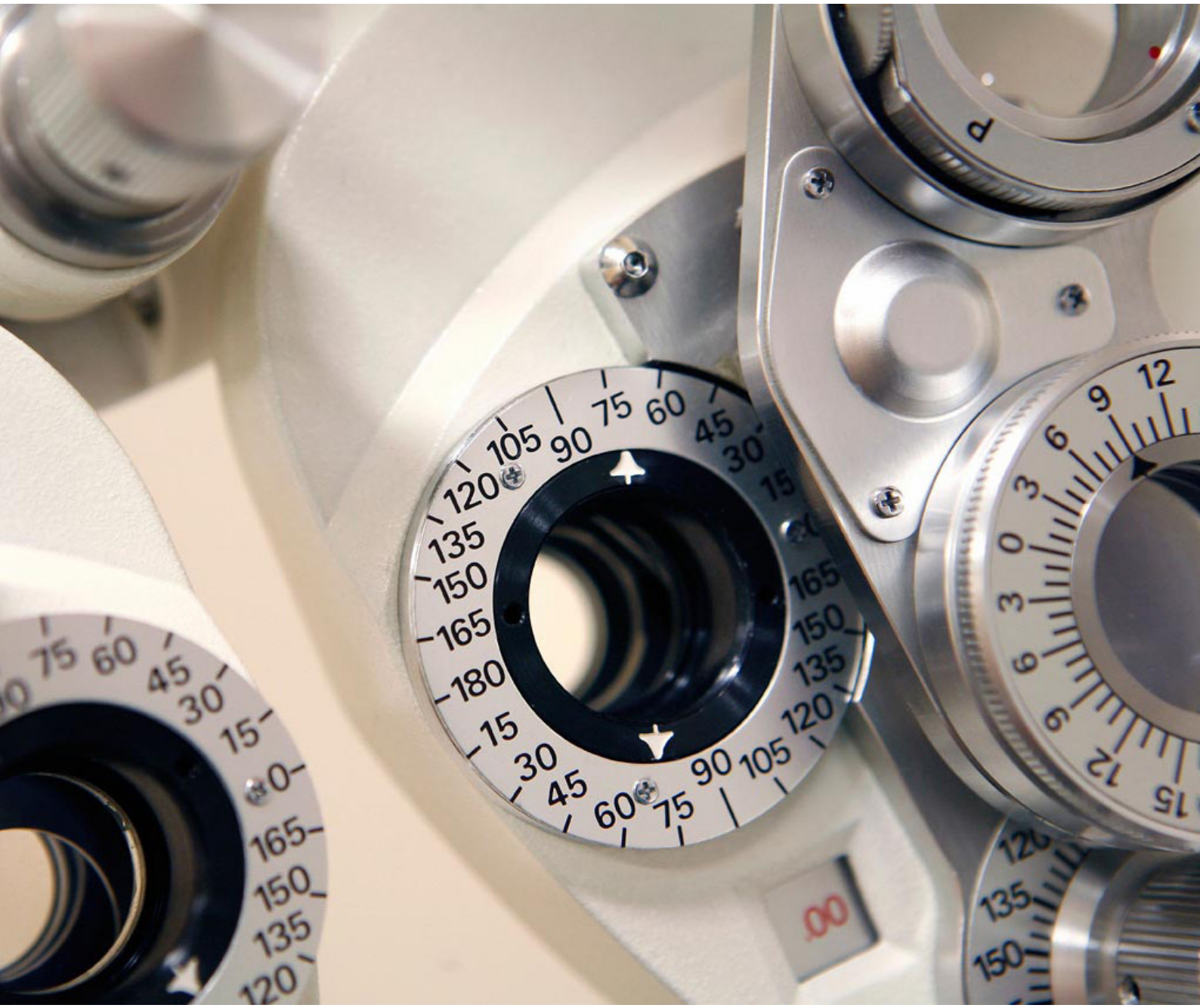
Our general conclusion identifies an increase in network-connected medical devices and, thus, in the cyber risks for medical devices. The risk of viruses disrupting medical devices was mentioned most. In addition, the following attention points are noted:

- Almost a quarter of the hospitals state to have an explicit policy in place for data security of medical devices;
- More than half the hospitals state to have been affected by a computer virus in their medical devices;
- Less than a quarter of the hospitals state to be sure network-connected medical devices use encryption;
- More than three-quarters of the hospitals state it is not possible (generally) to directly encrypt data of a medical device and store it on USB sticks;
- Slightly less than three-quarters of the hospitals has adequate procedures in place to remove data from medical devices before they are removed.

Preventing incidents (both as a result of targeted and random attacks) is crucial. Nevertheless, no longer using the many innovative solutions offered by healthcare technology is not the right path to follow. Network segmentation, NAC, SOC and SIEM solutions can mitigate the threats for existing medical devices. Privacy and security should be factored in right from the start for new medical devices. This is how the countless possibilities new technologies have to offer can be used safely.

Word of thanks

Without the support of the hospitals we would never have been able to perform this research. We wish to extend a warm thank you to everyone involved. What's more, the report would not have been possible without the efforts of Tom-Martijn Roelofs, Salo van Berg, Derk Wieringa, Marrit Plat and Marko van Zwam.



Literature consulted

1. United States Government Accountabillity Office, '*Medical Devices – FDA Should Expand Its Consideration of Information Security for Certain Types of Devices*', 2012, http://www.gao.gov/assets/650/647767.pdf, geraadpleegd op: 20-01-2015.
2. Nederlandse Zorg Autoriteit, Medische specialistische Zorg – weergave van de markt 2009-2013, 01-12-2013, http://www.nza.nl/104107/105773/742312/Marktscan_medisch_specialistische_zorg_2013.pdf
3. U.S. Department of Health and Human Services/Office of Inspector General, Work plan for Fiscal Year 2014, http://docs.ismgcorp.com/files/external/OIG-Work-Plan-2014.pdf
4. Nationaal Cyber Security Centrum, Cybersecuritybeeld Nederland 4, 10-07-2014, https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-4.html
5. Wired/Kim Zetter, It's Insanely Easy to Hack Hospital Equipment, 04-25-2014, http://www.wired.com/2014/04/hospital-equipment-vulnerable/
6. U.S. Food and Drug Administration, Content of Premarket Submission for Management of Cybersecurity in Medical Devices, 02-10-2014, http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
7. College Bescherming Persoonsgegevens, Onderzoek naar de beveiliging van het netwerk van het Groene Hart Ziekenhuis, 06-10-2014, https://cbpweb.nl/sites/default/files/atoms/files/rap_2014_netwerkbeveiliging-groene-hart-ziekenhuis.pdf
8. Reuters/Jim Finkle, U.S. Government probes medical devices for possible cyber flaws, 22-10-2014, http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022
9. U.S. Department of Health and Human Services/Office of Inspector General, Work plan for Fiscal Year 2015, http://oig.hhs.gov/reports-and-publications/archives/workplan/2015/FY15-Work-Plan.pdf
10. College Bescherming Persoonsgegevens, CBP Agenda 2015, 28-01-2015, https://cbpweb.nl/nl/nieuws/cbp-presenteert-toezichtagenda-voor-2015