ISSN 1831-9424

European Commission

Cyber security in the health and medicine sector: a study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings

Reina, V., Griesinger, C.

2024

Joint Research Centre

EUR 32014

Contact information
Name: Vittorio Reina
Address: Via E. Fermi, 2749 I – 21027 Ispra (VA) ITALY
Email: vittorio.reina@ec.europa.eu
Tel.: +39 0332 78 3638

EU Science Hub
https://joint-research-centre.ec.europa.eu

JRC138692

EUR 32014

PDF ISBN 978-92-68-19790-5 ISSN 1831-9424 doi:10.2760/693487 KJ-NA-32-014-EN-N

Luxembourg: Publications Office of the European Union, 2024

How to cite this report: European Commission, Joint Research Centre, Reina, V. and Griesinger, C., *Cyber security in the health and medicine sector: a study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings*, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2760/693487, JRC138692.

Contents

Abstract

The health and medicine sector are increasingly digitized, a trend that will accelerate with more widespread adoption of artificial intelligence, wearables and internet of things-based healthcare. Yet, this digital transformation carries notable cybersecurity threats. While there is ample evidence on cyberattacks to this sector, information on whether they cause health impacts is contradictory, in particular whether they have, subsequently, contributed to severe health outcomes.

In order to explore this inconsistency, we used the Europe Media Monitor (EMM) to retrieve media content on cyber incidents in healthcare settings reported in several European languages over one year. We focused on cyber incidents with reported impact to patients' health by using selected combinations of keywords and appropriate exclusion criteria. We retrieved 21 cyber incidents with potential health impacts such as postponed therapies, delayed surgeries. Notably, for none of the incidents adverse health effects (e.g. injury, deterioration of health, death) were reported.

This study reveals cyber vulnerabilities in the EU healthcare sector and further highlights the challenge of characterising cyber incidents in regard to their health consequences. Hurdles are a lack of consistent evaluation and reporting criteria and a lack of frameworks for assessing causality. We alert that such tools need to be developed in order to prepare for the rising risk of cyber incidents in an increasingly digitised healthcare environment.

Acknowledgements

We would like to acknowledge the JRC colleagues Arianna Galli for setting up and monitoring Europe Media Monitor (EMM) results and Eleonora Mantica for the support in using EMM.

Authors

Vittorio Reina

Claudius Griesinger

1 Introduction

In contrast to many other sectors, cyber-attacks to healthcare facilities have the potential not only to degrade the quality and timeliness of health services but also to endanger the health and the life of patients. For example, under a worst-case scenario, an urgent operation that cannot be conducted because of a cyber-attack on the cloud storage facility of the patient's imaging files or involving a required robotic surgery tool, could even lead to the serious deterioration of the health or death of that patient. Unfortunately, the **lack of preparedness and investment in robust cybersecurity measures, the usage of legacy information systems (i.e. that is not any more cyber secure) and other reasons intrinsic to the area, leaves the healthcare and wider health sector with significant vulnerabilities and gaps in cyber protection**.

However, characterising cyber incidents in health and assessing their effects on patients' health is difficult for various reasons. For instance, health effects due to postponed and rescheduled treatment could happen with a significant delay, posing considerable challenges for detecting a causal connection. In addition, hospitals may be reluctant to provide this type of information due to potential conflicts of interest or fear or reputational damage. Finally, there are no agreed methodologies for characterising health cyber security incidents and for monitoring possible causal associations with adverse health effects. Consequently, there are only few studies available that have reported and/or quantified possible health impacts resulting from cyber incidents. Some notable studies are outlined briefly below:

- Choi et al. (2019) analysed the 30-day fatality rates for acute myocardial infarction (AMI) in U.S. hospitals. The authors found that, from 2011 to 2017, the fatality rate dropped on average 0.4% each year due to progress in care. However, in hospitals where data breaches occurred, the fatality rate increased 0.34–0.45% per year for 2–3 years. While these figures appear small, if translated in patient numbers, it exposes a significant number of individuals to substantial health risks.

- The Ponemon Institute, a respected IT security research organization released reports in 2022([1]) and 2023([2]) entitled "The Insecurity of Connected Devices in Healthcare" and "Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care", respectively. The first report is based on data provided by 517 healthcare experts in leadership positions at hospitals and healthcare facilities throughout the US and the second presents the outcomes of a survey of 653 healthcare IT and security practitioners in the US. **In 2022 56% of respondents say their organizations experienced one or more cyberattacks in the past 24 months involving IoMT/IoT devices. In 2023 88% of organizations experienced at least one cyber-attack over the previous 12 months.** In both years cyberattacks (e.g. supply chain attack, ransomware) were reported to have resulted in compromised patient care such as **impacted healthcare services including inappropriate therapy or treatment deliveries. Importantly, both reports indicated increased in mortality** rates as a consequence of cyberattacks.

However, these reports and findings are in contrast to the rather limited number of cyberattacks that received widespread public attention and which reported direct impacts on patients' health:

([1]) In partnership with Cynerio: https://www.cynerio.com

([2]) Sponsored by Proofpoint: https://www.proofpoint.com

- **Possible fatal consequence due to delayed treatment:** In 2020 a female patient scheduled to undergo critical care([3]) in Dusseldorf, Germany died in hospital during an ongoing ransomware attack and subsequent network outage affecting the hospital. However, German police ultimately concluded that a "causal link" between the attack and the patient's death could not be established beyond doubt.
- **Possible perinatal complications:** In 2020: a mother sued an U.S. hospital after the death of her baby which had been born with a nuchal cord (i.e. a condition where the umbilical cord is wrapped around the baby's neck). The mother argued that this led to brain damage and, a few months later, the baby's death([4]), alleging that doctors had failed to carry out critical pre-birth testing due to a cyberattack on the hospital.
- **Possible treatment errors:** In 2022 an overdose of opioids was given to a 3 year old boy while recovering from tonsillectomy([5]) in a US hospital. When the boy received post-operative treatment, the hospital experienced a cyber-attack which blocked access to online medical records and resorting to manual procedures for dosing relevant medication.

Major attack on a national health system: The Health Service Executive (HSE) is the publicly funded healthcare system in the Republic of Ireland. It is responsible for the provision of Ireland's public health services in hospitals and communities across the country. In May 2021 HSE was subject to a very sophisticated ransomware cyber-attack that impacted all of the HSE's national and local systems involved in all core services. The impact was so huge that the HSE cyber-attack was recently defined as the *«landmark event of its type in Ireland»*([6]). The independent review "Conti cyber-attack on the HSE Independent Post Incident Review" (HSE, 2021) commissioned by HSE analysed in detail relevant technical/organisational aspects of that attack. However, even if the magnitude of the attack, there is very little information on possible health impacts[7]. Related to the same cyber incident, (Moore et al., 2023) describes the response of health service staff to the loss of ICT systems. To do that, representatives from services in these sites most affected by the cyber-attack were invited to participate in focus groups to share their experiences and learning. While there was no evidence that healthcare provision in the immediate aftermath of the attack has resulted in harm to patients, clinical staff suspected that they will not be fully aware of the impact of mitigations on patients treated during this period for a long time to come.

Taken together, there is a clearly a discrepancy in the literature and in media reports concerning whether and to which extent cyber incidents in healthcare settings may lead to adverse consequences on patients' health. While there is a Cyber Incident Tracer #HEALTH([8]) providing a

---

([3]) https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital

([4]) https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

([5]) https://www.dailymail.co.uk/news/article-11312413/Des-Moines-hospital-claims-cyber-attack-blame-boy-3-given-MEGADOSE-opioids.html

([6]) https://www.itpro.com/security/ransomware/the-hse-cyber-attack-was-a-landmark-event-in-ireland-has-it-learned-from-the-experience

([7]) «For some oncology patients in the middle of treatment, the Incident meant that hospitals didn't have access to the patient's radiotherapy plans and could not safely continue treatment without new medical imaging. Some hospitals used adjacent private facilities where available, to take new medical images to continue providing radiotherapy treatment to patients»

([8]) https://cit.cyberpeaceinstitute.org/

collection of cybersecurity incidents in healthcare and medicine, the tracker does not collect information on magnitude and impact on health.

In order to address this discrepancy and data gap, we used the Europe Media Monitor (EMM) tool to scan the Internet for one year, from the 1st of May 2022 to the 30th of April 2023 to **retrieve news, in several EU languages, on cyber incidents in Europe with possible health impacts.** Our primary objective was to assess whether there is and the quantity of information on incidents a) with significant potential health impacts (e.g. delayed treatment) and b) to determine whether there were reports that indicated consequences on patients' health (e.g. death, deterioration of health). Our study therefore had a different aim than that of the ENISA report "Threat Landscape: Health Sector" (ENISA, 2023) which focused on gathering quantitatively all incidents in healthcare settings in the EU.

Our search was conducted for media publishing in English, German, Italian, French and Spanish. It therefore did not cover all languages spoken in the EU and the results may not be representative for the entire European Union. If there is an error, it is an error of underestimation of incidents. However, the findings do provide insights into cyber incidents occurring in major EU economies.

2 Europe Media Monitor (EMM)

EMM was initiated in 2002 as a project to support the European Commission with its media monitoring activities. The main purpose of EMM is to monitor a predefined set of media sources, reduce the information flow to manageable proportions by applying categorisation and extract additional metadata like entities, quotes, sentiment/tonality, geo-location, etc.

EMM supports users in their need to monitor the most up-to-date information, detect threats, follow trends and analyse impacts. It enhances the EU's prevention, preparedness and response capabilities to a wide range of threats (e.g. humanitarian crises, natural and man-made disasters, endangerment of public health, conflict, terrorism and organised crime). It is also used by communication units to create press reviews and assess reputation of their own institutions.

The EMM engine feeds news articles through several specialized processing nodes that analyse the text, extract relevant metadata and perform categorization. NewsBrief([9]) and MedISys([10]) (Medical Information System, specific for public health risks) are two public web sites, fed with EMM metadata, that display breaking news and short-term trends, early alerts and up-to-date category-specific news.

At the moment, the publicly accessible instance of EMM monitors over 44 000 RSS feeds/ HTML pages from almost 13000 media websites in more than 70 languages and retrieves and processes around 300 000 new news articles per day. These articles are categorized into over 9 000 categories. A selected subset of these categories and the results of the clustering process can be seen on the public EMM website http://emm.newsbrief.eu. It runs 24 hours per day, 7 days a week.

Typical users of EMM are EU institutions and agencies, national authorities of EU Member States, international organisations (e.g. African Union, World Food Program) and the general public (over 30,000 Internet users per day access the publicly available web sites).

More information on EMM is available at https://knowledge4policy.ec.europa.eu/online-resource/europe-media-monitor-emm_en

2.1 The EMM categorisation System

The main component that determines the information streams from EMM is a powerful keyword-based categorisation system. The category definitions allow for word/weight lists, Boolean combinations, proximity and character wildcards. Each category definition consists of a list of customized keywords designed to select desired news and, eventually, of a list of excluded keywords to ignore news not relevant. When the news is selected, a reference to the news is placed into the appropriate category. The system deals efficiently with overlapping categories and it is not based on any hierarchical category structure. The system also covers languages such as Arabic (first character after whitespace is not the first character of the noun) and ideograph languages such as Chinese (no whitespace).

When the category is defined, it forms a core of the alert system that analyses the full text of the news articles, not just the headline and the abstract; it scans the entire text and tags those news

([9]) http://emm.newsbrief.eu

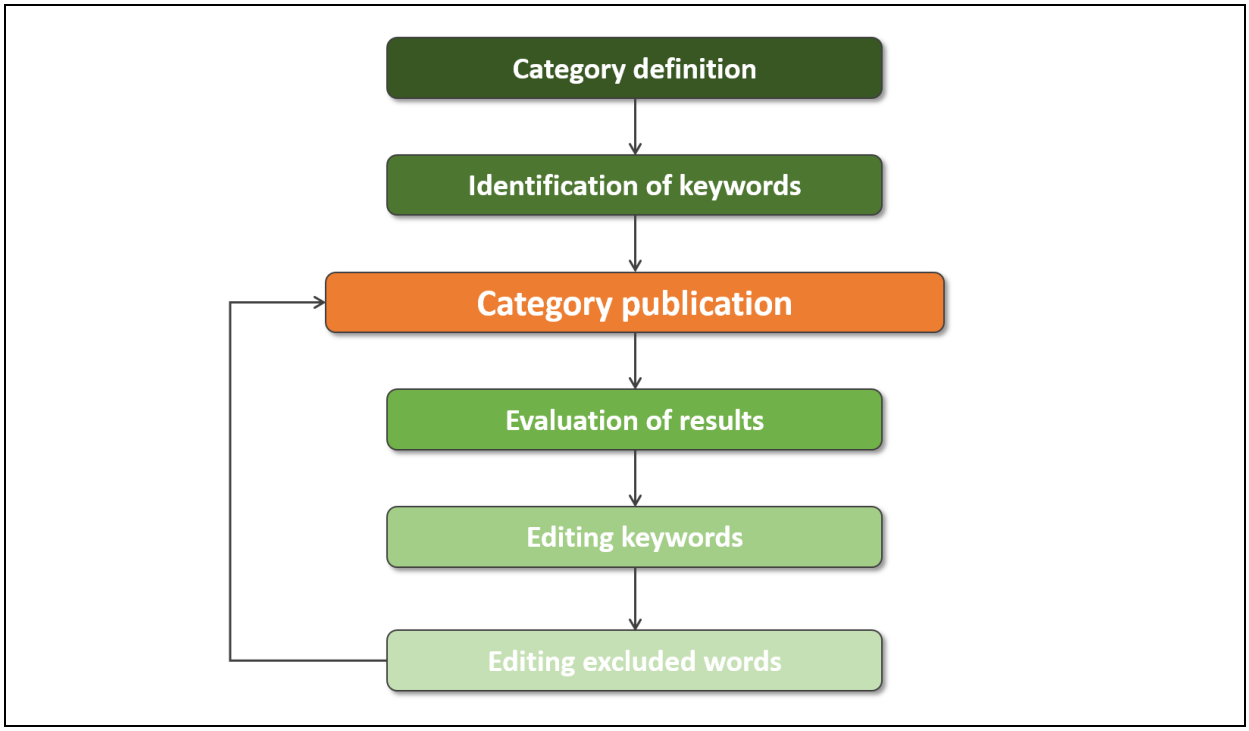
([10]) http://medisys.newsbrief.eu MEDISYS is an instance of EMM specifically developed for internet bio-surveillance and is used by a number of Health Agencies.

matching the selected keywords. The system runs continuously, scanning and checking all new published news articles against multi-lingual lists of keywords.

Given its features, we identified EMM as the proper tool for detecting news concerning cyber incidents in healthcare and medicine. In fact, traditional media (e.g. online newspapers) and also specific websites (e.g. https://thehackernews.com, https://www.redhotcyber.com) possibly report on cyber incidents occurred as a consequence of adversarial attacks. By defining appropriate keywords, these news may be detected and reported by EMM.

To test the capacities of the EMM and to find optimal combination of keywords to achieve our objective, we created several categories. Before launching the operational phase, we refined these categories over a period of 3 months, including the keywords used and by evaluating and cross-checking the relevance of identified news articles. The evaluation/refinement procedure is depicted in Figure 1. It should be noted that, when necessary, we implemented some modifications to the categories (e.g. new exclusion words) also during the monitoring period (from the 1st of May 2022 to the 30th of April 2023).

Figure 1. Refinement procedure of keyword lists



Source: own production

We initially created three categories focused on medical devices and specific cybersecurity issues:

- *MedicalDevices-Cybersecurity*
- *MedicalDevices-Cybersecurity-Privacy*
- *MedicalDevices-Cybersecurity-Ramsomware*

After the evaluation period, we decided to use a single category in several languages able to retrieve the majority of relevant news in one place: *MedicalDevices-Cybersecurity-Health.*

In the next chapters we describe these categories and the process we followed to create them.

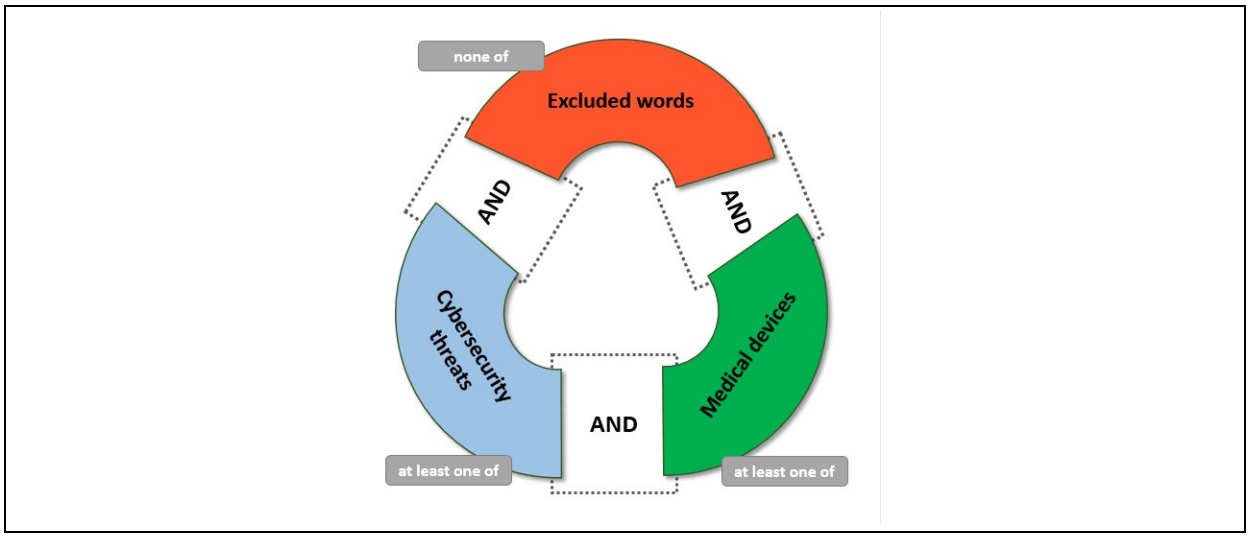
2.1.1 Categories MedicalDevices-Cybersecurity / Privacy / Ransomware

At the beginning of this activity, we created three categories: one focused on medical devices and cybersecurity and other two dedicated to specific cybersecurity aspects (i.e. privacy and ransomware)

MedicalDevices-Cybersecurity

The objective of the first categories we created, was to retrieve news on medical devices and generic cyber security issues (e.g. cyber-attacks, vulnerabilities). Following the procedure illustrated in Figure 1, and after one month of tests, the category was structured as shown in Figure 2 where each coloured area is a set of keywords.

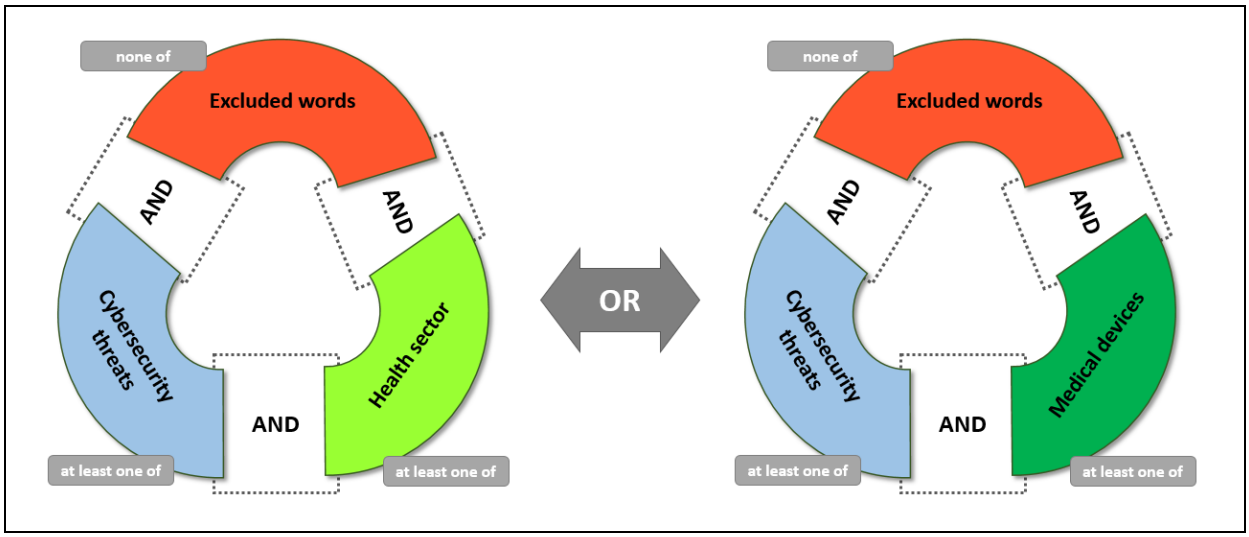
Figure 2. First version of the category *MedicalDevices-Cybersecurity*



Source: own production

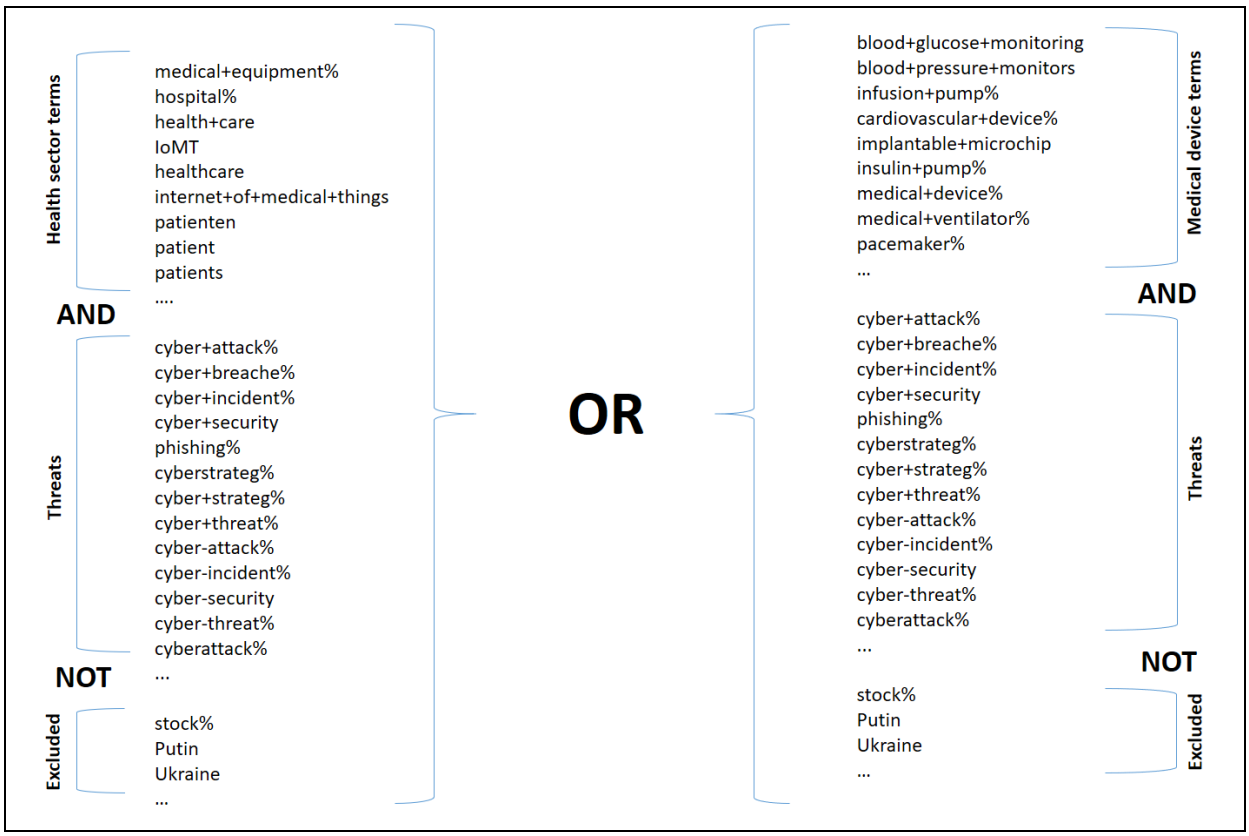
In the second iteration of the refinement process we decided to add a second combination including a set of keywords dedicated to the health sector (e.g. hospital, patient) in order to increase and improve the quality of the results obtained. The structure of the final version of the category and an extraction of keywords are presented in Figure 3 and in Figure 4.

Figure 3. Structure of the category *MedicalDevices-Cybersecurity*



Source: own production

Figure 4. Examples of keywords of the category *MedicalDevices-Cybersecurity*



Source: own production

MedicalDevices-Cybersecurity-Privacy and MedicalDevices-Cybersecurity-Ramsomware

In parallel we decided to test the possibility to use other two categories, focused on medical devices and two specific aspects related to cybersecurity:

- *MedicalDevices-Cybersecurity-Privacy*
- *MedicalDevices-Cybersecurity-Ramsomware*

Their structure was similar to the first version of the category *MedicalDevices-Cybersecurity* illustrated in Figure 2 where the block *Cybersecurity threats* was replaced with a block with specific keywords for privacy (e.g. data security breach) and ransomware (e.g. ransomware) respectively.

After two months of monitoring, we decided to abandon the approach of using multiple specific categories because we noticed a considerable overlap between their results.

2.1.2 Category MedicalDevices-Cybersecurity-Health

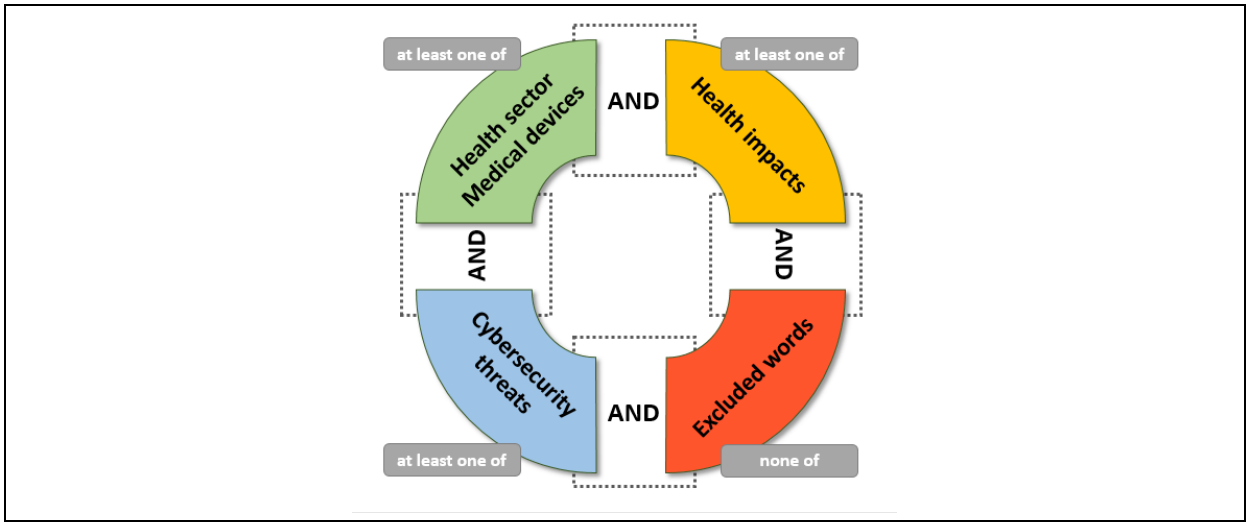
As described in the previous chapter, after two months of testing and monitoring the three initial categories, we decided to create a unique category with **the addition of a new set of keywords related to possible health impacts caused by cyber-attacks** (e.g. therapy disruption, delay of treatment) **to address the main objective of this report**. The new category was named *MedicalDevices-Cybersecurity-Health* to differentiate it from the first we created (see 2.1.1). Its structure is illustrated in Figure 5.

Additionally, in order to have a broader set sources, we added keywords in other 4 languages than English: Italian, Spanish, French and German. The relation between the keywords in the different languages is shown in Figure 6.

In Figure 7 it is presented an extract of English keywords. The full list of keywords for all the languages is available in Annex 1.

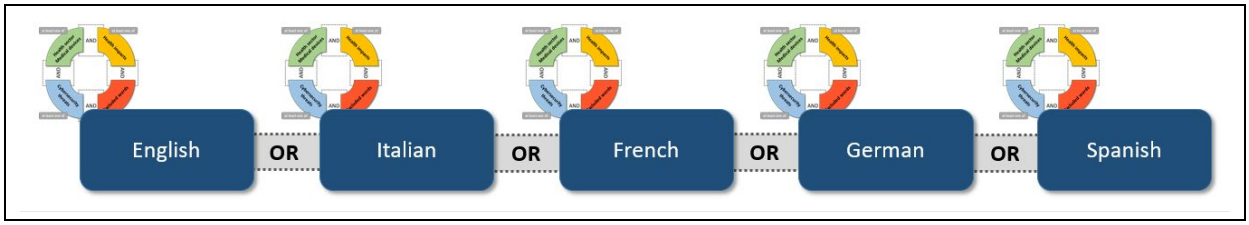
MedicalDevices-Cybersecurity-Health is the category that we used to carry-out the objective of this report. The results we obtained are described in Chapter 3.

Figure 5. Structure of the category *MedicalDevices-Cybersecurity-Health* for one language



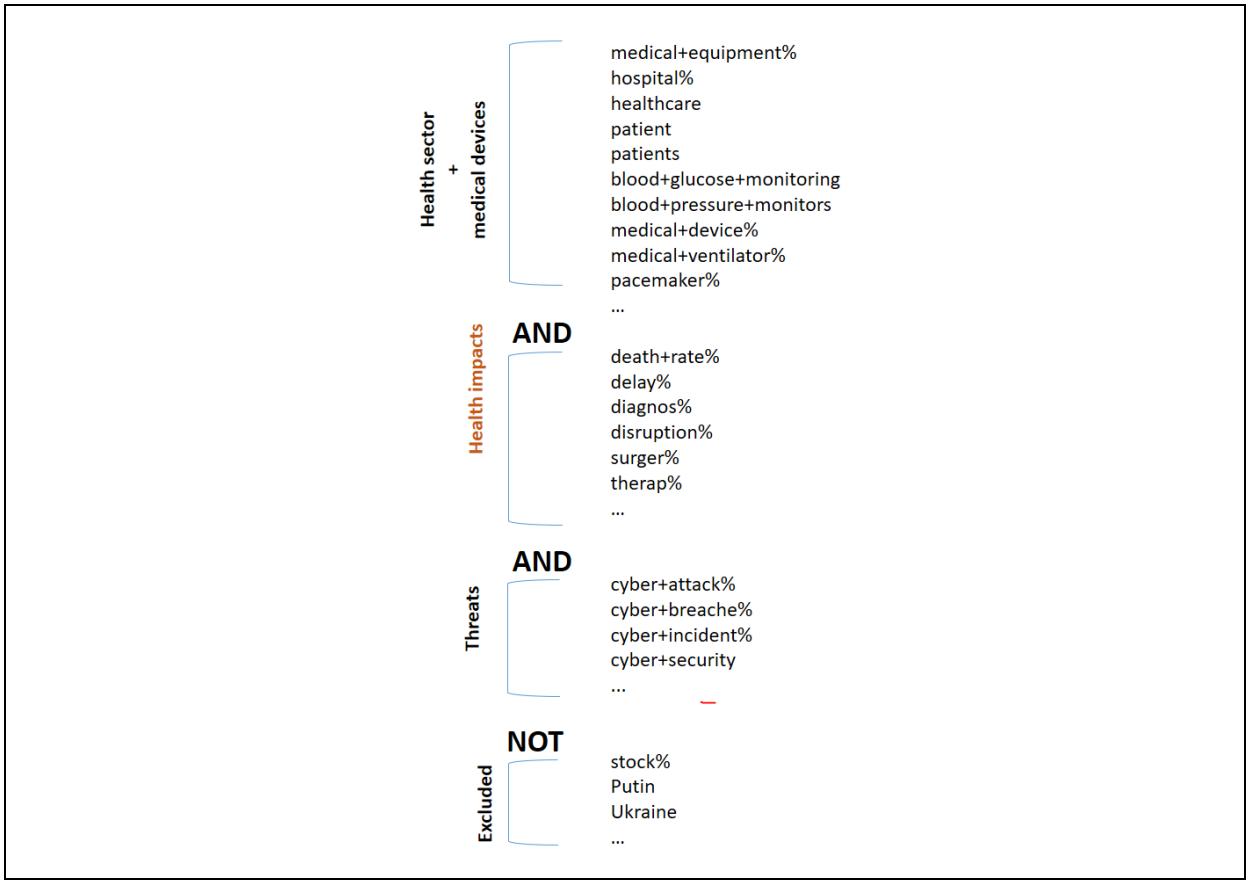
Source: own production

Figure 6. Relation between the keywords in different languages of the category *MedicalDevices-Cybersecurity-Health*



Source: own production

Figure 7. Examples of English keywords of the category *MedicalDevices-Cybersecurity-Health*



Source: own production

3 Results

The EMM category *Medical Devices-Cybersecurity-Health* retrieved many news that have been evaluated one by one in order to identify the most relevant for our objective. We evaluated both news articles reporting a new cyber incidents and, in order to identify possible health impacts, also follow-up news of ongoing or resolved cyber incidents. As an example of the quantity of the news retrieved, solely the combinations of keywords in German fetched 664 news articles. Finally, we identified **21 cyber incidents to European healthcare or medicine infrastructure/facilities that could potentially impact patients' health** (see Table 1).

Fortunately**,** based on the information retrieved, **none of these appeared to have caused direct health consequences in patients** (e.g. injury, illness, death). According to the description of the incidents selected, the main impacts on healthcare services and thus patients were the following:

- Therapies postponed
- Surgeries delayed
- Ambulances diverted away from attacked facilities
- Limited access to emergency rooms (ER)

We found that hospitals were the main targets with 20 selected cyber incidents and the remaining incident affected a distributor of medicine. The majority of cyber incidents were reported in Italy and France, but it is challenging to determine why these two countries had higher numbers than the others. One possible explanation could be the occurrence of **waves of attacks** that affected France during the period under consideration similarly as happened in non-European countries such as New Zealand([11]), Costa Rica and India([12]) in the same period. Another factor to consider is the specificity of our search. Since **our focus were cyber incidents causing health impacts, the keywords we used were configured to capture such incidents** excluding incidents having other targets, such as non-medical IT systems, patient data or health services. Consequently, certain types of attacks, like data theft, might not have been included in our findings, leading to lower numbers for some countries. For the same reasons, attacks that targeted institution and organisations such as Health Authorities, Health Insurance Companies or Health Research Entities might not have been detected. Finally, higher numbers could also indicate a lower level of awareness for cyber threats and, consequently, a lower level of cyber protection and mitigation measures in place.

Figure 8 presents the distribution of these 21 cyber incidents by type of attacks utilised and by country respectively. Concerning the type of attacks, it is immediately visible that **ransomware was the favourite choice by threat actors**.

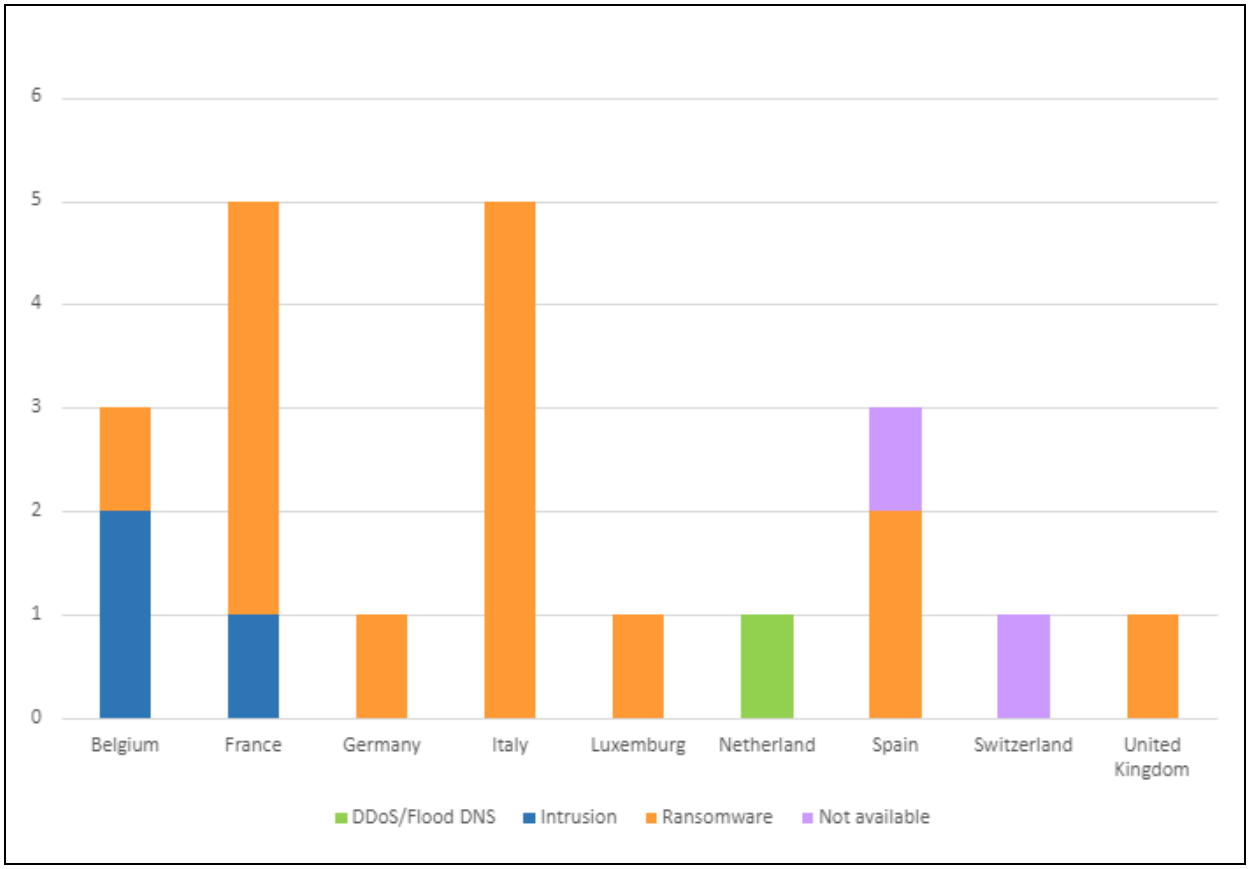
Cyber threats in healthcare settings have been previously described in the relevant deliverables of the PANACEA project (D2.1 2019) and by (ENISA, 2023). According to (ENISA, 2023) the type of attacks underlying relevant threats can be defined as follows:

([11]) https://tech.hindustantimes.com/tech/news/after-ireland-massive-ransomware-attack-now-shuts-down-new-zealand-hospitals-71621939809045.html

([12]) https://www.thehindu.com/sci-tech/technology/cyber-attacks-on-indian-healthcare-industry-second-highest-in-the-world-cloudsek/article65914129.ece

- **Ransomware** is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability and confidentiality.
- **Denial of Service** threats and attacks have availability as target. Among them DDoS (Distributed Denial of Service) stands out. DDoS attacks target system and data availability and, though not a new threat, have a significant role in the cybersecurity threat landscape of the health sector.
- **Intrusion** refers to incidents where an attack on a system has been confirmed or made public and attackers have gained access to systems but the details of how the breach or intrusion took place are not clear.

Figure 8. Type of cybersecurity incidents by country



Source: own production

The results of a similar project are presented in (ENISA, 2023). It should be noted however that the ENISA report covers a wider time frame (from January 2021 to March 2023), includes a broader range of targets (e.g. Health Insurance Companies, Laboratories) and encompasses a wider scope of affected assets (e.g. patient data). Importantly, the ENISA study, in contrast to our study, did not focus in detail on health consequences / adverse events in patients. There are also methodological differences: ENISA gathered the list of incidents based on Open-Source INTelligence (OSINT) and

ENISA's own Cyber Threat Intelligence (CTI) capabilities([13]) which crawl various sources such as CTI providers, institutional stakeholders, social media, data feeds, cybersecurity news, vulnerability disclosure, academia and deep/dark web. In contrast, our study employed JRC's EMM tool, which focuses on media reports. Not surprisingly, the ENISA study identified a larger number of incidents (n=215) and found a greater variety of cyber incidents.

That being said, when we restrict the incidents in (ENISA, 2023) to the same time frame and similar affected assets (i.e. healthcare services and citizens/patients), we find that both results are within the same order of magnitude.

([13]) More information available in the *ENISA cybersecurity Threat landscape Methodology* at https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

Table 1. List of cyber incidents to European healthcare or medicine infrastructure/facilities that could potentially impact patients' health

Date	Country	News	Impact	Follow Up	Data leak	Type of incident
01/05/2022	Italy	Milano, hacker attack to 4 Hospitals: Fatebene Fratelli, Sacco, Buzzi and Melloni	Limited access to the Emergency Room. No access to patient medical records and to radiology exams and blood sampling.	Ransomvare ViceSocitey. 2022-06-28: Data Breach. After 10 days the major issues have been solved	Yes	Ransomware
05/05/2022	Italy	Lombardia ATS Insubria Varese3 and Como: cyberattack	Online services not available (e.g. mammography screening)	2022-05-10: ATS website is still ko.2022-05-23: end up on the web incomes and addresses of 800 disabled serious. After 50 days the services are back to normality.	Yes	Ransomware
14/05/2022	Luxembourg	Hôpitaux Vivalia	All consultations (except exceptions which will be communicated directly to patients) are canceled. Emergency operations, which do not require the laboratory, will be maintained.	After two weeks, it seems that the ransom has been paid because Vivalia disappeared from the Lockbit website	Not proved. Hackers threatened to publish.	Ransomware
20/05/2022	Belgium	Belgium: Lockbit ransomware attack to Arlon and Bastogne hospitals	Almost all non-emergency operations have been canceled. "Except for exceptions judged according to criteria of necessity and urgency, in consultation between doctors, nurses and the medical director", notes Vivalia. With a few rare exceptions, consultations have also been cancelled. The attaque is strictly connected with the one to Vivalia. Luxemburg is worried.	n.a.	No	Ransomware

Date	Country	News	Impact	Follow Up	Data leak	Type of incident
20/06/2022	Switzerland	Swiss: hacker attack to the H+ hospitals	Online servicecs not available. Details of the impacts not available.	n.a.	No	N.A.
21/06/2022	Italy	Ospedale Macedonio Melloni di Milano	No information regarding disruption of services (only data breach)	n.a.	Yes	Ransomware
18/08/2022	France	French Hospitals hit by ransomware attack	Hospital's business software, the storage systems (in particular medical imaging), and the information system relating to patient admissions inaccessible. Patients in need of emergency care will be evaluated by CHSF's doctors, and if their condition requires medical imaging for treatment, they will be transferred to another medical center.	Return to normal operations by the end of October (2 months and a half)	Yes	Ransomware
19/08/2022	Italy	Torino: ASL hit by ransomware attack	On August 24th, the management of the health company published a new press release listing the services that remain active (First Aid, outpatient visits, hospitalizations and hospital visits and surgical interventions) while the collection of radiological reports can only take place at the Secretariats of Radiology.	On 6 October, 95% of data had been restored	Partial data exfiltration	Ransomware

Date	Country	News	Impact	Follow Up	Data leak	Type of incident
01/09/2022	United Kingdom	Britannic Hospital NHS hit by ransomware attack	Home visits cancelled, doctors making clinical decisions without access to patient notes, and a huge backlog of paperwork. Sources warning that some regions already face a six-month backlog of a “few hundred thousand” patient care notes that would need to be manually processed.	After 3 weeks the initial attack against NHS staff continued to take care notes with “pen and paper”. According to the media reports found, the effect on patient healthcare were lasted at least three weeks. The company stated that it might take another 12 weeks to get some services back online.	The company did not disclose whether any NHS patient data had been compromised or whether it was negotiating with the hackers.	Ransomware
07/10/2022	Spain	Catalan hospitals: ransomware attack	Staff cannot view records, schedule, or perform tests that depend on the system, such as X-rays.	After three weeks the process of restoration is still ongoing	Yes	Ransomware
09/10/2022	France	Maternity hospital in Paris	Administrative tasks are slower. Usual e-mails do not work. Reduce its reception capacity in the birthing room, which is a centralized monitoring system of babies’ vital functions.	n.a.	Yes Criminal hackers had exfiltrated patients’ personal data, including health data	Ransomware

Date	Country	News	Impact	Follow Up	Data leak	Type of incident
15/11/2022	France	CEntre Saint-Jean	From November 15 to 18, 2022, its chemotherapy and radiotherapy activities for which access to the computerized patient file is essential (ballistics, dosages, reports, etc.). All treatments resumed in partnership with the Guillaume-de-Varye private hospital (*). But they had to stop the radiotherapy treatments. All the nearby centers helped to take care of the patients who needed it.	Around three weeks	No	Ransomware
29/11/2022	Germany	Klinikum Lippe	According to the clinic, there was a partial failure of the IT systems following a massive hacker attack. Internally, IT systems are available or have been reverted to the former analog form, for example for food orders. The care of patients in hospital and emergency patients remains guaranteed at all times because they quickly switched to analogue procedures for patient care. The clinic's locations can only be reached by telephone and fax. There is still no (public) information about the perpetrators.	After one week, the Lippe Clinic negotiated with the blackmailers and received the data necessary to decrypt the systems. It is not known whether or how much ransom was paid.	No	Ransomware

Date	Country	News	Impact	Follow Up	Data leak	Type of incident
05/12/2022	France	Hôpital André-Mignot du centre hospitalier de Versailles	Limited reception of patients. The hospital has launched its white plan, partially deprogrammed operations and is doing everything possible to maintain outpatient care for its patients and consultations.	More than two weeks after being targeted, the hospital has still not returned to its usual functioning.	No	Ransomware
25/01/2023	France	Lyon hospitals	Some surgeries had to be postponed other day after the attack.	The normal program was able to resume two days later.	No	Attempt of intrusion
01/02/2023	Netherlands	Dutch Hospitals	Dutch cyber authorities said Wednesday that several hospital websites in the Netherlands and Europe were likely targeted by a pro-Kremlin hacking group because of their countries' support for Ukraine. Only the publicly accessed section of its website had been affected by the attack.	n.a.	No	DDoS
05/03/2023	Spain	Barcelona Clinic Hospitals	Devastating cyberattack. Staff at the facility's laboratories, pharmacies and emergency services have been reduced to using pen and paper. Cancellation of surgeries and medical appointments.	n.a.	Yes	Ransomware

Date	Country	News	Impact	Follow Up	Data leak	Type of incident
10/03/2023	Belgium	Brest Clinic Hospital (Belgium)	The Internet information system was thus "isolated" in order to "limit the spread of the attack" and all CHRU communications with the outside world (making appointments, sending results, connections with other institutions, etc.) are therefore disrupted. But “emergency services are provided” and “no deprogramming is envisaged”, underlines the hospital, which can be reached by telephone at the usual number.	Gradually back to normality after two weeks (24/03/2023)	No	Intrusion
23/03/2023	Spain	Catalan pharmacies	Some pharmacists have been unable to use the online system. Delayed and even prevented the normal delivery of some medicines to pharmacies in Spain. Patient data is not at risk. Limited patient impacts.	n.a.	No	N.A.
11/04/2023	Belgium	Centre hospitalier de Bourg-en-Bresse	The cyberattack has no impact on patient reception. All hospital activities are insured.	n.a.	n.a.	Intrusion

Date	Country	News	Impact	Follow Up	Data leak	Type of incident
21/04/2023	Italy	Multimedica Milano	Enormous inconvenience for patients, who saw outpatient clinics and the emergency room go into chaos, as well as the delivery and collection of clinical analysis reports. Impossible to take X-rays, deliver reports and also access medical records.	After the first “break-in” which took place in the night between Friday 21 and Saturday 22 April, a new attack took place on Tuesday 25 April. All outpatient activity, the Emergency Department and the collection of reports were suspended. Only obstetrics, dialysis, rehabilitation, chemotherapy, nuclear medicine and hospitalization activities were guaranteed. After 3 weeks the systems had been restored and the situation was back to initial status	No	Ransomware

Source: own production

4 Conclusions

Although there is a substantial amount of new articles and a sizeable amount of scientific publications on (types of) cyber incidents targeting healthcare facilities, there is a notable discrepancy in regard to whether and to which extent cyberattacks affect the health of patients due to the fact that there is considerable variation and inconsistency concerning the characterisation of cyber incidents and potential health-related consequences.

In order to address this discrepancy and potential data gap, we used, from the 1st of May 2022 to 30th of April 2023, the Europe Media Monitor (EMM) to retrieve news on cyber incidents in healthcare settings reported in several European languages. Based on the consistent application of search strategies and exclusion criteria, we identified 21 cyber incidents (covered by several reports in some instances) which mentioned potential health impacts on patients related to deteriorated care provision (e.g. delayed surgery). For none of these incidents, direct adverse consequences on patients' health were reported.

The main impacts were:

- Therapies postponed;
- Surgeries delayed;
- Ambulances diverted away from attacked facilities;
- Limited access to emergency rooms.

Ransomware was the cyber-attack type most frequently used. Of the 21 incidents retrieved, 20 concerns hospitals and one a supplier of medicinal products. As a consequence of the attacks, hospitals were often obliged to redirect ambulances and relocate patients in need of surgery to other nearby hospitals. This finding is in line with a study by McGlave et al. (2023). In this kind of scenarios, attacks to hospitals can be considered not only a local issue but also a "*regional disaster*"([14]).

In order to tackle in a timely fashion the effects of cyberattacks, e.g. by keeping systems up and running on the basis of a fall-back plan, various mitigation and preparedness measures are required that a collectively subsumed under the term "**cyber resilience"**. As stated in Moore et al. (2023) «***healthcare quality is the key outcome for resilience in healthcare***. *Healthcare quality includes clinical effectiveness,* ***patient safety****, timeliness, patient centeredness, care coordination, efficiency, and equity, and each of these dimensions was compromised during the cyberattack*» and «***preparedness is key for resilience***».

The **World Economic Forum**, in February 2024, advised that «*a collaborative and systemic approach within the ecosystem is key — cyber resilience must be viewed beyond just the confines of any one organization*». «*Building cyber resilience requires not only protecting individual entities but also ensuring the robustness of the entire ecosystem to withstand and recover from cyber incidents*»([15]).

([14]) https://www.npr.org/2023/06/25/1184025963/cyberattacks-hospitals-ransomware
([15]) https://www.weforum.org/agenda/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/

In this perspective, it is essential to identify **specific response actions and mitigation measures to cyber incidents**. In fact, as described in Nelson et al. (2022), «*each cyberattack and hospital setting is different. Different hospitals and departments may have unique vulnerabilities based on available technologies and the effect of any attack. Therefore,* ***there is no one-size-fits-all preparedness plan or solution****. Ultimately, each department will need to determine its specific vulnerabilities, risks, and available resources to* ***create an individualized preparedness plan for restoring patient care***».

Considering that **the average cyber-attack on a health care infrastructure results in a 19-day period during which patients are unable to receive some form of care/to access certain forms of care**([16]), technical (e.g. encryption, network segmentation) and non-technical (e.g. awareness, training and exercising) remedial actions should be supplemented with specific mitigation measures such as **contingency plans**. The report HSE NQPSD (2022) that analyses the clinical impact on patient safety of the cyber-attack on the Irish Health Service Executive (HSE) in May 2021, concludes that «*contingency planning should be viewed as an integral part of implementing healthcare ICT systems*» that «*will help to ensure that patient safety remains central to the delivery of care*».

One example of individualized preparedness plan is described in O'Shea et al. (2022). Medical physicists at University Hospital Galway and the National University of Ireland Galway initiated the development of an in-house tool to assist in creating radiotherapy treatment plans after cyber incident-induces interruptions. The tool, named EQD2VH, calculates treatment compensation plans and enables visual comparison of all plan options, as well as individual analysis of each structure in a patient's plan. Other examples of radiation oncology departments' responses and mitigations measures are presented in Yu et al. (2023) and Harrison et al. (2022) and Chen et al. (2021). In particular the authors of this paper, developed a four-phase recovery planning framework and created a helpful a high-level readiness checklist, demonstrating how to approach planning for significant downtime events. The example is based on a radiology system, but the findings can be adapted for contingency planning for other healthcare systems.

In regard to preparedness and cyber resilience, the PANACEA project, funded by the European Union's Horizon 2020 research and innovation programme, provides two useful instruments:

- a set of four models to describe the entity to be protected from cyber threats (Healthcare organizations, Medical Device Lifecycle, System Development Lifecycle) and the related security system (the Cybersecurity system) (PANACEA, D1.1 2019);
- the Cybersecurity Framework for healthcare, a valid toolkit that can support an effective roadmap for securing IT systems in the healthcare sector, making the most of existing security governance frameworks (PANACEA, D8.1 2022). This toolkit is structured in four phases:
    a. Analysis, aimed at assessing the status of the cybersecurity system and at identifying improvement interventions;
    b. Prioritization and planning, aimed at prioritizing the interventions (e.g. investments) and in defining an implementation plan;

([16]) https://cit.cyberpeaceinstitute.org/explore

c. Implementation, aimed at realizing the interventions;

d. Management, aimed at performing the required routine identification and protection, detection and, in case of attack, response and recovery activities.

Considering the "***wide, dynamic and vulnerable attack surface***" (PANACEA, White Paper 2021), the instruments just presented should be connected with several factors that critical infrastructure, such as public health facilities, should take into consideration when dealing with cyber security([17]):

- A **lack of supply-chain management**, controls, and policies in place, especially for vendors with access to critical infrastructure networks;
- The **lack of cybersecurity planning**, such as encryption, user privilege, password management, multi-factor authentication (MFA), and network segmentation;
- **Outdated software and legacy systems** that no longer receive security updates and vulnerability patches;
- **Insufficient cybersecurity awareness** among employees and staff;
- **Insider threats** from disgruntled employees, contractors, vendors, or individuals with access to critical systems can pose a significant risk to the integrity and security of these infrastructures;
- **IoT devices,** heavily used today in critical infrastructure, may bring **new attack surfaces and potential vulnerabilities** that threat actors may exploit.

If preparedness is important, **monitoring and characterising** cyber incidents are equally relevant activities. Based on the description of the incidents available in the news, it is evident that some of them were more serious than others. However, as stated in *ENISA (2023),* with the information we collected «*we cannot measure accurately the impact of delayed treatment and care to a patient's health*». Unfortunately, the lack of consistent evaluation and reporting criteria complicates the estimation of health impact.

We are convinced that it is necessary to further design and develop tools geared towards describing and assessing incidents in the health and medicine sectors, not only for reporting activities, but also to facilitate the implementation of adequate mitigation measures and to improve responsiveness to cyber incidents that may affect patient health. The development of tools specific to healthcare and medicine, such as a **cybersecurity ontology**, can be used for this purpose and fill this gap. In addition, there is a need for a robust framework for assessing potential causal connections between cyber incidents and adverse health effects. Without such tools, the increasing digitalisation of the healthcare sector will remain unmonitored and under-researched in regard to its cyber security related risks.

([17]) https://www.securityinfowatch.com/security-executives/article/53069429/why-critical-infrastructure-is-the-new-target

References

Chen P-H, Bodak R, Gandhi NS. Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. Journal of digital imaging. 2021; 34(3):731-40. DOI: 10.1007/s10278-021-00466-x

Choi S, Johnson ME. Do hospital data breaches reduce patient care quality? arXiv. (2019) 1904. DOI: 10.48550/arXiv:1904.02058

ENISA THREAT LANDSCAPE: HEALTH SECTOR, July 2023, https://www.enisa.europa.eu/publications/health-threat-landscape

Harrison Amy S., Sullivan Paul, Kubli Alex, Wilson Kathleen M., Taylor Amy, DeGregorio Nicholas, Riggs Joseph, Werner-Wasik Maria, Dicker Adam, Vinogradskiy Yevgeniy, How to Respond to a Ransomware Attack? One Radiation Oncology Department's Response to a Cyber-Attack on Their Record and Verify System, Practical Radiation Oncology, Volume 12, Issue 2, 2022, Pages 170-174, ISSN 1879-8500. https://doi.org/10.1016/j.prro.2021.09.011

HSE Board in conjunction with the CEO and Executive Management Team, Conti cyberattack on the HSE Independent Post Incident Review - 03 December 2021, https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

HSE NQPSD (2022) A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare ICT failure. Dublin: National Quality and Patient Safety Directorate (NQPSD) of the Chief Clinical Officers Office, Health Service Executive, https://www.hse.ie/eng/about/who/nqpsd/qps-intelligence/qps-intelligence-reports/cyber-study-report.pdf

McGlave, C. C., Neprash, H. & Nikpay, S. Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients. SSRN Scholarly Paper, 2023, 10.2139/ssrn.4579292

Moore, G., Khurshid, Z., McDonnell, T. et al. A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. BMC Health Serv Res 23, 1112 (2023). https://doi.org/10.1186/s12913-023-10076-8

Nelson Carl J., Soisson Emilie T., Li Puyao C., Lester-Coll Nataniel H., Gagne Havaleh, Deeley Matthew A., Anker Christopher J., Roy Lori Ann, Wallace H. James, Impact of and Response to Cyberattacks in Radiation Oncology, Advances in Radiation Oncology, Volume 7, Issue 5, 2022, 100897, ISSN 2452-1094. https://doi.org/10.1016/j.adro.2022.100897

O'Shea K, Coleman L, Fahy L, Kleefeld C, Foley MJ, Moore M. Compensation for radiotherapy treatment interruptions due to a cyberattack: An isoeffective DVH-based dose compensation decision tool. J Appl Clin Med Phys. 2022; 23:e13716. https://doi.org/10.1002/acm2.13716

PANACEA (Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people), D1.1 Models of health services and of medical device lifecycle for cybersecurity, 01/08/2019, https://www.panacearesearch.eu/deliverables/d11-models-health-services-and-medical-device-lifecycle-cybersecurity

PANACEA (Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people), D2.1 Analysis of cyber vulnerabilities and SoA countermeasures in HCC, 30/04/2019, https://www.panacearesearch.eu/deliverables/d21-analysis-cyber-vulnerabilities-and-soa-countermeasures-hcc

PANACEA (Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people), D8.1 PANACEA Security Framework for Hospitals and care centres, 28/02/2022, https://www.panacearesearch.eu/sites/default/files/PANACEA_Deliverable_D8.2%20v1.1_0.pdf

PANACEA (Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people), White Paper, Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres , December 2021, https://www.panacearesearch.eu/sites/default/files/WhitePaperA4_December2021_final_0.pdf

Ponemon Institute, Cynerio, The Insecurity of Connected Devices in Healthcare, 2022, https://www.cynerio.com/ponemon-survey-insecurity-of-connected-devices-in-healthcare-2022

Ponemon Institute, Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care 2023, https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

Yu James B., Dicker Adam P., Lester-Coll Nataniel H., Tsai C. Jillian, Zawalich Matthew, Practical Steps to Mitigate Cybersecurity Attacks on Radiation Oncology Practices, Practical Radiation Oncology, 2023, ISSN 1879-8500, https://doi.org/10.1016/j.prro.2023.05.001

List of abbreviations and definitions

Abbreviations	Definitions
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Cybersecurity
EMM	Europe Media Monitor
HSE	Health Service Executive (Ireland)
IoMT	Internet of Medical Things
IoT	Internet of Things

List of figures

List of tables

Annexes

Annex 1. Full list of keywords for EMM category *Medical Devices-Cybersecurity-Health*

English	
At least one of	
	CT+scanner% IoMT X-ray+computed+tomography aortic+stent% aortic+valve% arteriograph artificial+cardiac+pacemaker% artificial+joints artificial+leg% artificial+limb% asthma+spacer% automated+external+defibrillator balloon+catheter% bioartificial+liver+device% blood+glucose+monitoring blood+pressure+monitors blood+sugar+meters bone%+implant% bypass+cardiopulmonar% cardiac+device% cardiopulmonary+bypass cardiovascular+device% cardioverter% cardioverter+defibrillator% catheter% defibrillator% defibrillator+surgery endoscopic+device% health+care healthcare heart+pump% heart+valve% hospital% implantable+microchip implanted+cardioverter-defibrillator implanted+pulse+generator incentive+spirometer infusion+pump% insulin+pump% insulinpumpe internet+of+medical+things laparoscopic+device% medical+device% medical+equipment% medical+implant% medical+infusion+pump% medical+ventilator% microchip+implant% minimally+invasive+device% neural+stimulator% neurological+device% neurostimulator% ophthalmoscope orthopedic+device% otoscope

	pacemaker% patient patients pneumograph prostehetic+device% rehabilitation+device% respiratory+device% health sphygmomanometer% stethoscope% surgical+instrument% surgical+robot% tissue+engineered+device% ultrasound+endoscope valve%+cardiaque% vascular+stent%
AND at least one of	
	cyber-strateg% cyber+attack% cyber+breache% cyber+incident% cyber+security phishing% cyberstrateg% cyber+strateg% cyber+threat% cyber+vulnerabilit% cyber+risk% cyber-attack% cyber-incident% cyber-security cyber-threat% cyberattack% cybercriminal% cybercrime+attack% cybersecurity cyberthreat% cybervulnerabilit% hacker% hacking+incident% security+breach% security+vulnerabilit% security+vulnerabilities malicious+software malicious+activit% ransomware% ransomware-related anti-ransomware% malware% WannaCry cyber+vulnerabilities killware%
AND at least one of	
	brain+damage% attack% death% died death+consequenc% death+of+a+patient death+rate% death+toll delay%

	diagnos% ransom% pay% paid disrupt% patient+care% health+risk% heart+attack%+death% baby%+death impact+on life-or-death+consequenc% infant%+death life-threatening+implication% mortality+rate% patient%+death patient+has+died patient+s+death patient+to+death patient+who+died safety+at+risk% safety+issue% surger% therap% transfer% treatment% undiagnos%
BUT none of	
	Putin Zelensky stock% Ukraine blockchain geopolitic% management+market% market%+research market%+opportunit% shoot-out tirote% shoot%

OR

Italian
At least one of
agenzi_+regional_+di+sanità aziend_+sanitar% clinica+ospedaliera cliniche+ospedaliere dispositiv_+medic_ ospedal_ pazient_ sanità serviz_+ospedalier_ servizi%+sanitar% sistem_+sanitar% strument_+diagnostic_ strument_+medic_ unità+local+socio+sanitari%

	nosocomi_ clinicamente ambulatori_ anestesia diagnostic% degenz_ cardiologi% pediatri% neonat% trapiant% Usl Asl Ats
AND at least one of	
	attacc%+hacker hacker% attacc%+informatic_ crimin%+informatic_ cyber+attacc% cyber+criminal_ cyberattacc% cybercriminal_ malware pirat_+informatic% ramsomware sicurezza+informatica anti-malware anti-ramsomware cybersecurity cyberterroris% spyware phishing firewall firmware
AND at least one of	
	raggi-x bloccare dati+sanitari+in+pericolo bloccat_ blocco conseguenz_+fatal_ raggi+x conseguenze+gravi dann_ radiograf% parali% dannos_ risonanz_ riscatt_ paga% disservizi disservizio gravi+conseguenze gravi+disagi mort_ mortal_ ritard_ in+tilt uccidere anamnesi cartell_+clinic%

OR

French	
At least one of	
	dispositifs+médicaux défibrillateur+automatique dispositif+medic hôpital hospital% hôpitaux patient patients santé système+sanitaire services+de+santé surdiagnostic pédiatri% hospitalisation cardiologi%
AND at least one of	
	cyber+attaque% cyberattaque% cyber-attaque% cyber-sécurité cyber+sécurité rançongiciel cybersécurité cybercrime cybersecurity ransomware cybercriminalité cybersurveillance cyberdéfense cybercriminel_ hacke% pirat% cyberterroris% malveillant% spyware malware firewall firmware phishing
AND at least one of	
	diagnostic% réhospitalisation récupération retard résonance+magnétique paralys% urgence% vers% salair% cardiogramme risque+pour+la+santé résonance thérapie

	radiographie traitement

OR

German	
At least one of	
	gesundheit% krankenhaus Krankenhäuser patienten sanitäres+system geduldig
AND at least one of	
	cyber+angriffe onlinesicherheit online-sicherheit cyber-security cyber+security cybersecurity hacker%
AND at least one of	
	diagnose verzögern wiederherstellung hospitalisiert therapie behandlung

OR

Spanish	
At least one of	
	dispositivos+médico% clínic% hospital% industria+de+la+atención+médica organizacione%+de+atención+médica organizacione%+de+salud industria+de+salud sistema%+hospitalarios sistema%+de+salud servicio%+de+salud servicio%+sanitario% sector%+de+la+salud sector%+sanitario% sector%+medico% paciente%

AND at least one of	
	ciberseguridad ciberamenaza% ciberriesgo% cibercriminal% ciberdelincuente% criminale%+cibernético% ataque%+cibernético% pirata%+informático% intrusione% incidente%+cibernético% ciberataque% seguridad+cibernética riesgo%+cibernético% hackeo% hackeado brecha%+de+seguridad amenaza%+cibernética% seguridad+del+dispositivo%
AND at least one of	
	interrump% aplaza% postpuest% cancel% fatal% retras% cirugías diagnostica_ murió deceso_ muert% tasas+de+mortalidad terapia_ tratamiento% dosis mortal% prestación% diagnóstico% impacto%+negativo% operacione%+clínica% denegación inactividad afect%
BUT none of	
	asesin% explosiv% ejército militar% armada_ tirote% pistoler% soldad% shoot%

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

— at the following standard number: +32 22999696,

— via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

EU Science Hub
Joint-research-centre.ec.europa.eu

Publications Office
of the European Union