KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

imec

Cybersecurity of medical devices: Legal and ethical challenges

Elisabetta Biasin & Erik Kamenjasevic
Centre for IT & IP Law (CiTiP) – KU Leuven

Cybersecurity Initiative Flanders Seminars
Thursday, 16 July 2020, 12:30 - 13:30
Jitsi Meet

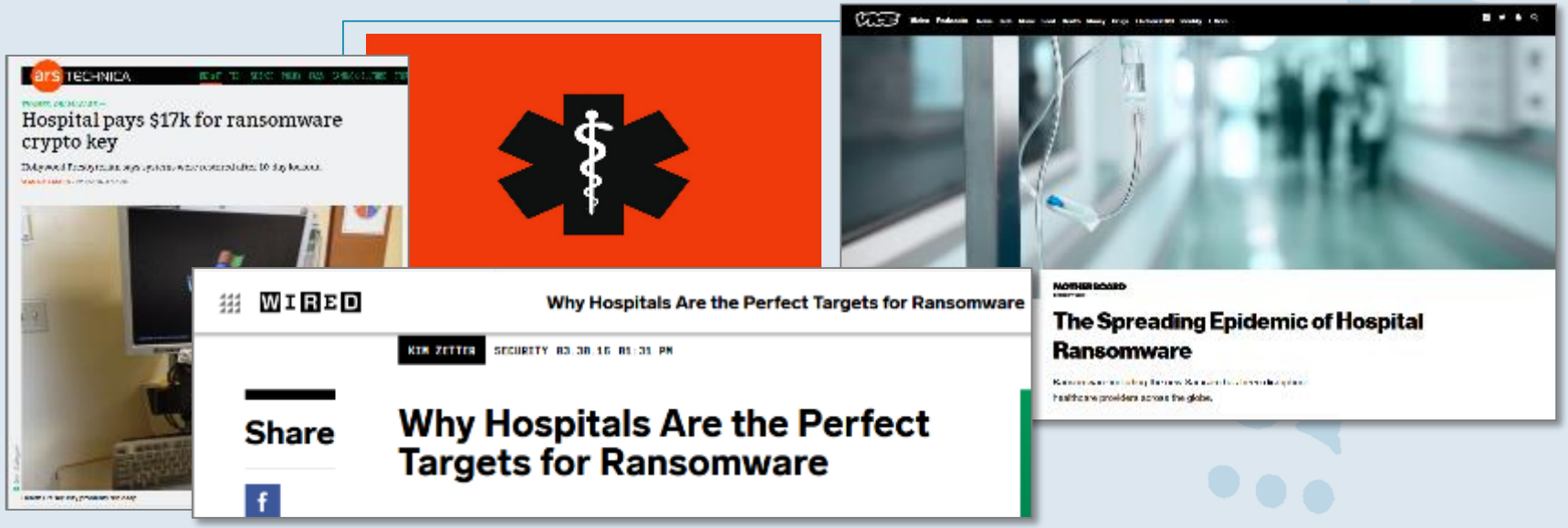
Content

- Introduction
- Laws concerning cybersecurity of medical devices
- Regulatory challenges
- Ethical Concerns beyond the legal framework
- Other examples
- Annex

Introduction

Cybersecurity in the healthcare sector (1/2)

- Definition
- Wannacry and Petya triggered discussions – amongst practitioners, healthcare professionals, policy makers and legislators – on the security of healthcare infrastructures, and how to enhance them



Introduction

Cybersecurity in the healthcare sector (2/2)

- Since 2010, an exponential growth of **connected-to-network** medical devices. As a consequence, higher exposure of their vulnerabilities to cyber-attacks.
- In the US, this has been regulated by FDA since 2014. In the EU?

The EU agenda for cybersecurity

EU initiatives to promote NIS security

The EU Cybersecurity Strategy (2013)
The EU Cybersecurity Package (2017)
The NIS Directive (2016)
The Cybersecurity Act (2019)
ENISA reinforcement
Commission Recommendation on Cybersecurity of 5G Networks (2019)

EU laws concerning cybersecurity of connected medical devices

Ensuring cybersecurity of medical devices implies application of several legal instruments:

- ***NIS Directive***
- ***Cybersecurity Act***
- ***GDPR***
- ***MDR***
- ***RED***

NIS Directive

Personal and material scope

Network and Information System

a) an **electronic communications network**

b) any **device** or group of interconnected or related devices which perform **automatic processing of digital data;**

c) digital data stored, processed, retrieved or transmitted by elements under points (a) and (b) for the purposes of their operation, use, protection and maintenance

Security (of NIS)

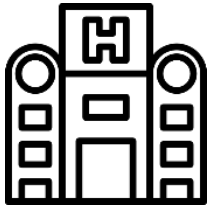
The **ability** of network and information systems **to resist**, at a given level of confidence, **any action that compromises the availability, authenticity, integrity or confidentiality** of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

NIS Directive

Personal and material scope

Operators of Essential Services

- public or private entities that **have to be identified by every Member State**.
- Conditions:
  - (1) they provide a **service** 'which is essential for the maintenance of critical societal and/or economic activities' **which**
  - (2) **'depends on network and information systems**' where
  - (3) an incident on the latter would have a 'significant disruptive effect on the provision of that service'.



The **type of entity considered as essential services operators** are '**Healthcare providers**' (= 'means any natural or legal person or any other entity legally providing healthcare on the territory of a Member State'); i.e., **hospitals**

NIS Directive

Personal and material scope

Security Requirements

Operators of essential services must take **appropriate measures** to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

… as part of these security requirements

Notification obligations for OES

Operators of essential services must **notify,** without undue delay, the **competent authority** or the national **Computer Security Incident Response Team (CSIRT)** of incidents having a significant impact on the continuity of the essential services they provide.

Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident.

Cybersecurity Act

Personal and material scope

2 objectives:

- ✓creation of a framework for European Cybersecurity Certificates of ICT products, processes, and services.
  - Obtaining a certificate is voluntary, and vendors can decide themselves whether they would like their products to be certified.

- ✓strengthening the role of the EU Cybersecurity Agency (ENISA).

7.6.2019 EN Official Journal of the European Union L 151/15

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 17 April 2019
on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Network and information systems and electronic communications networks and services play a vital role in society and have become the backbone of economic growth. Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and, in particular, support the functioning of the internal market.

(2) The use of network and information systems by citizens, organisations and businesses across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the internet of Things (IoT) an extremely high number of connected digital devices are expected to be deployed across the Union during the next decade. While an increasing number of devices is connected to the internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In that context, the limited use of certification leads to individual, organisational and business users having insufficient information about the cybersecurity features of ICT products, ICT services and ICT processes, which undermines trust in digital solutions. Network and information systems are capable of supporting all aspects of our lives and drive the Union's economic growth. They are the cornerstone for achieving the digital single market.

(3) Increased digitisation and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats and exacerbating the dangers faced by individuals, including vulnerable persons such as children. In order to mitigate those risks, all necessary actions need to be taken to improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses – ranging from small and medium-sized enterprises (SMEs), as defined in Commission Recommendation 2003/361/EC (4), to operators of critical infrastructure – are better protected from cyber threats.

(1) OJ C 227, 28.6.2018, p. 86.
(2) OJ C 176, 23.5.2018, p. 29.
(3) Position of the European Parliament of 12 March 2019 (not yet published in the Official Journal) and decision of the Council of 9 April 2019.
(4) Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Cybersecurity Act

Personal and material scope

- *Medical devices manufacturers* → medical devices may fall under the definition of ICT product: an "element of a network of information systems."
- *Healthcare providers* → inasmuch they use ICT processes or ICT services to carry out their activities.
- To obtain cybersecurity certification, manufacturers or healthcare providers may, voluntarily (if not obliged by national/EU law), apply to the conformity assessment bodies of their choice established in the Union.

GDPR

Personal and material scope

- ❖Sets obligations to ensure the security of the processing of data, which often happens in the context of connected-to-network medical devices.
- For processing of personal data → **technical and organizational measures** that are adequate to the risk of such processing.
  - In the case of networked medical devices, the role of a controller could involve healthcare providers, healthcare professionals, manufacturers of medical devices, and other users.

MDR

Personal and material scope

The MDR provisions primarily address *manufacturers of a medical device.*

"The natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured, or fully refurbished and markets that device under its name or trademark".

MDR

Personal and material scope

No explicit reference to cybersecurity of medical devices, but:

- MD has to meet the general safety and performance requirements set in Annex I

General requirements:

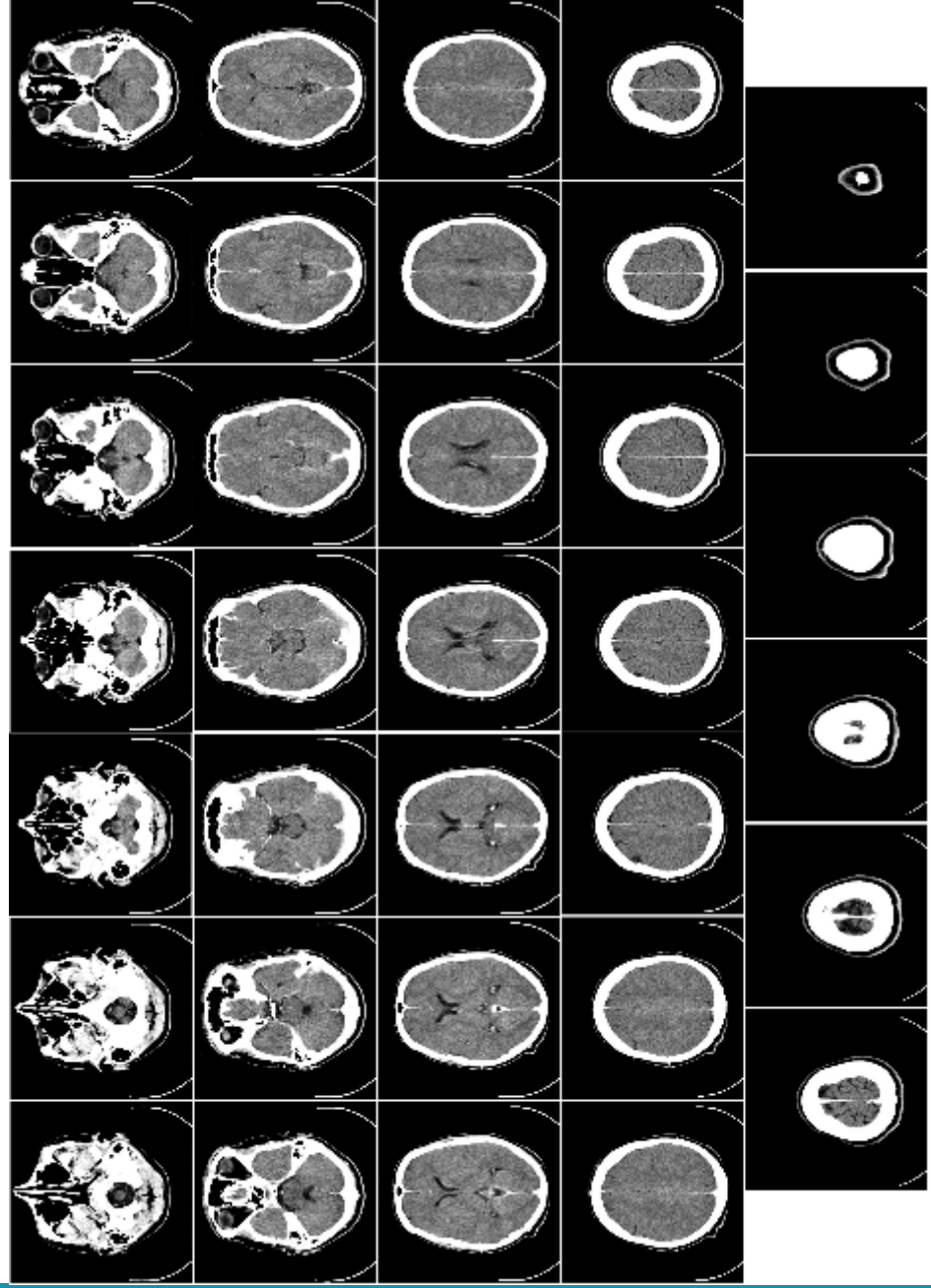
- Achieve the performance intended by the manufacturer and be designed in a way suitable for the intended use
- Be safe and effective, and associated risks shall be acceptable when weighed against the benefits of the patients and level of protection of health and safety while taking into account state of the art
- Establish and maintain a risk management system

MDR

Personal and material scope

MD designed to be used *with other devices*:

- have to be safe and should not impair the specified performance of the device
- shall be designed and manufactured in a way to remove, as far as possible, risks associated with possible negative interaction between software and IT environment within which they operate
- if they are intended to be used with another device, they shall be designed, so the interoperability and compatibility are reliable and safe



MDR

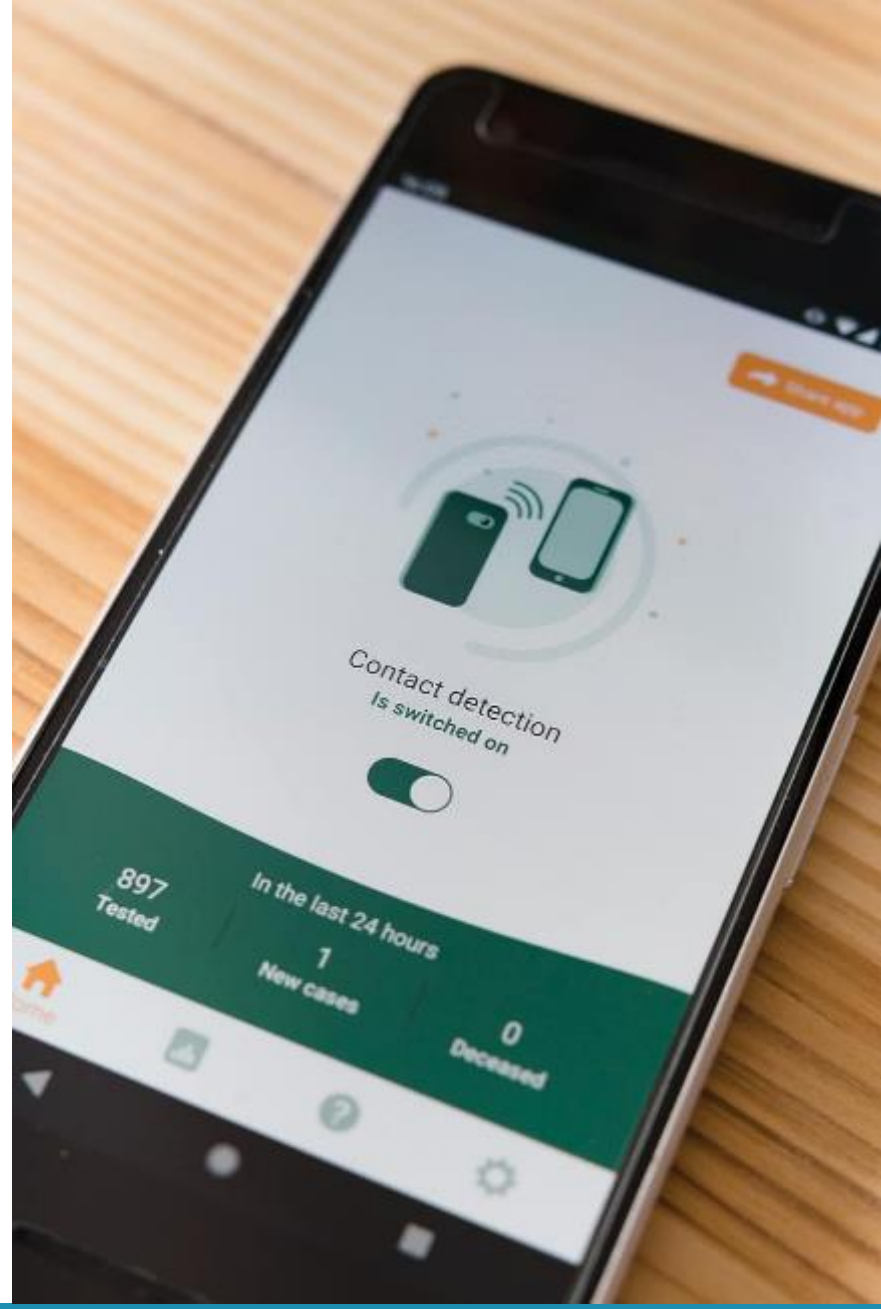
Personal and material scope

MD incorporating *software*:

- shall be designed to ensure repeatability, reliability, and performance according to the intended use, and appropriate means have to be adopted to reduce risks or impairment of the performance

- should be developed and manufactured according to the state of the art and by respecting the principles of the development life cycle, risk management (including information security), verification, and validation.

- manufacturers shall set out minimum requirements concerning hardware, IT network characteristics, and IT security measures (including protection against unauthorized access)



MDR

Personal and material scope

Other obligations:

- MD for use *by laypersons* shall be designed and manufactured so the layperson can use it according to his/her skills and the means available to him or her
- *Information* to be supplied together with the device: manufacturers must inform about residual risks, provide warnings requiring immediate attention on the label and, for electronic programmable system devices, give information about minimum requirements concerning hardware, IT networks' characteristics and IT security measures (including protection against unauthorized access), necessary to run the software as intended.

RED

Personal and material scope

- An “electrical and electronic product, which intentionally emits and/or receives radio waves for radio communication and/or radio determination.”
- Sets essential requirements for safety and health, electromagnetic compatibility, and the efficient use of radio spectrum.
- Foresees technical features for the protection of privacy, personal data, misuse, interoperability, and compliance regarding the combination of radio equipment and software.
- Requires building the radio equipment in a way which does not harm the network or its functioning, it does not misuse network resources and incorporates safeguards to ensure the protection of privacy and data protection of users and subscribers.

Regulatory challenges

Sections

1. Cybersecurity and its conceptualisation
2. Consistency requirements
3. Horizontal consistency requirements
4. Vertical consistency requirements
5. Horizontal and vertical consistency

Regulatory challenges

Cybersecurity and its conceptualisation

Conceptualisation of

- 'cybersecurity' has seen a **long-standing debate** (Kasper & Antonov 2019, Schatz et al 2017);
- cybersecurity aspects: seem **not to be coherent amongst regulators and policy-makers** in the EU (Fuster & Jasmontaite, 2020) SEE NEXT SLIDE

"*The **possibility of attaching different meanings to the term 'cybersecurity'** has both advantages and disadvantages. It indicates the flexibility of the term that can adapt to changing circumstances. At the same time, an ever-evolving term can become overly inclusive or broad in a manner that **would obstruct coherent regulation** in this area and in this way **hamper the development of regulatory measures***". (id.)

Regulatory challenges

Cybersecurity and its conceptualisation

Table 5.1 Definitions of cybersecurity in national cybersecurity strategies of EU Member States

Document title, country, year	Definition
Austrian Cyber Security Strategy, 2013	The term 'cyber security' stands for the security of infrastructure in cyber space, of the data exchanged in cyber space and above all of the people using cyber space.
Croatian Cybersecurity Strategy, 2015	Cyber security encompasses activities and measures for achieving the confidentiality, integrity and availability of information and systems in cyberspace.
Czech Republic Cybersecurity Strategy for the period of 2015–2020	Cyber security comprises a sum of organisational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyberspace in the Czech Republic for the benefit of both public and private sectors, as well as for the general public.
Cybersecurity Strategy of the Republic of Cyprus: Network and Information Security and Protection of Critical Information Infrastructures, 2012	Cybersecurity refers to the broader security of networked systems that operate in cyberspace, i.e. in most cases connected to the internet, and this term also covers the safe and secure usage of these systems by end users.
Dutch National Cyber Security: Strategy from awareness to capability, 2018	Cyber security is the entirety of measures to prevent damage caused by disruption, failure or misuse of ICT and how to recover should damage occur.
Estonian Cyber Security Strategy, 2014–2017	Cyber security is an integral part of national security; it supports the functioning of the state and society, the competitiveness of the economy and innovation.
Finland's Cyber security Strategy, 2013	Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured.
Italian National Strategic Framework for Cyberspace Security, 2013	With the term cyberspace, we refer to the complex of all interconnected ICT hardware and software infrastructure, to all data stored in and transferred through the networks and all connected users, as well as to all logical connections however established among them. It therefore encompasses the internet and all communication cables, networks and connections that support information and data processing, including all mobile internet devices.
Cyber Security Strategy for Germany, 2011	Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the internet as a universal and publicly accessible connection and transport network, which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.
Hungarian Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary, 2013	Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace.

(continued)

Table 5.1 (continued)

Document title, country, year	Definition
Cyber Security Strategy of Latvia, 2014–2018	Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
Lithuanian Cyber Security Strategy, 2011–2019	Electronic information security equates to cyber security.
Luxembourg Cybersecurity Strategy, 2015	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user assets. Organisation and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user assets against relevant security risks in the cyber environment.
Malta, National Cyber Security Strategy, Green Paper, 2015	Cybersecurity "is the safeguards and actions that can be used to protect cyber domain from those threats that are associated with or that may harm its interdependent networks and information infrastructure. It strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."
Cyberspace Protection Policy of the Republic of Poland, 2013	Cyberspace security—a set of organisational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace.
Cyber Security Concept of the Slovak Republic for 2015–2020	Cyber security is one of the defining elements of the security environment of the Slovak Republic and a subsystem of national security. At a state level, it is a system of continuous and planned increasing of political, legal, economic, security, defence and educational awareness, also including the efficiency of adopted and applied risk control measures of a technical-organisational nature in cyber space in order to transform it into a trustworthy environment providing for the secure operation of social and economic processes at an acceptable level of risks in cyber space.
National Cyber Security Strategy of Spain, 2013	Cyber security is a necessity of our society and our economic model.
UK National Cyber Security Strategy, 2016–2021	'Cyber security' refers to the protection of information systems (hardware, software and associated infrastructure), the data on them and the services they provide from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system or accidentally, as a result of failing to follow security procedures.

Source: Fuster & Jasmontaite, in The ethics of cybersecurity, CC BY 4.0

Source: Pixabay

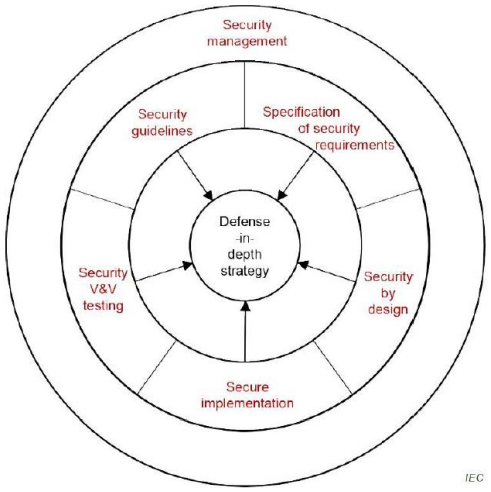
Regulatory challenges

Cybersecurity and its conceptualisation

MDCG Guidelines

Security-by-design

(Recital 12 CSA)



Security-by-default

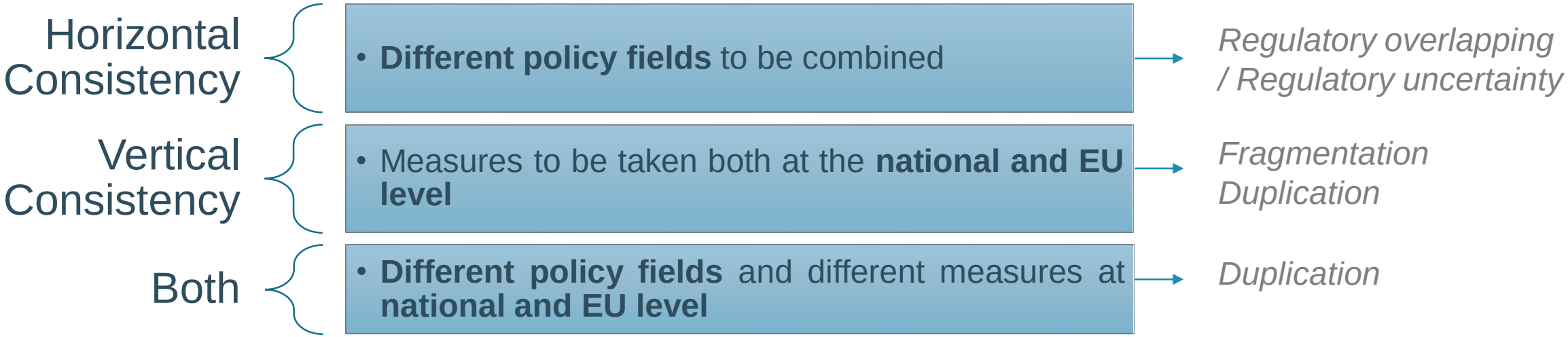
(Recital 13 CSA)

Joint responsibility

- Joint or shared responsibility?
- Actors involved?
- IMRDF vs MDCG

Regulatory challenges

Consistency requirements



Cybersecurity forms "*an excellent example of an area in which the different policy fields need to be combined (a requirement for **horizontal consistency**), and where measures need to be taken at the level of both the EU and Member States (calling for **vertical consistency**)*" (Wessel, 2015)

Regulatory challenges

Horizontal consistency requirements

Overlapping

Requirements

- Medical Devices Certification
- Cybersecurity Act Certification Schemes

Issue

A specific certification scheme not necessary (COCIR 2019)

Rec.

Clarify CSA scope
(for medical devices (excl), and for health devices (incl))

Pietro Jeng on Unsplash

Regulatory challenges

Horizontal consistency requirements

Uncertainty

Requirements

- Medical Devices Regulation Security Requirements
- Radio-Equipment Directive Security Requirements

Issue

Manufacturers autonomy vs requirements/ law scrutiny

Rec.

EU Regulators should provide more specific guidance

Autonomy for manufacturers: particularly relevant for health apps (!)
(Minssen et al. 2020; Kamenjasevic et al 2020; Biasin & Kamenjasevic)

Pietro Jeng on Unsplash

Regulatory challenges

Vertical consistency requirements

Fragmentation

Requirements

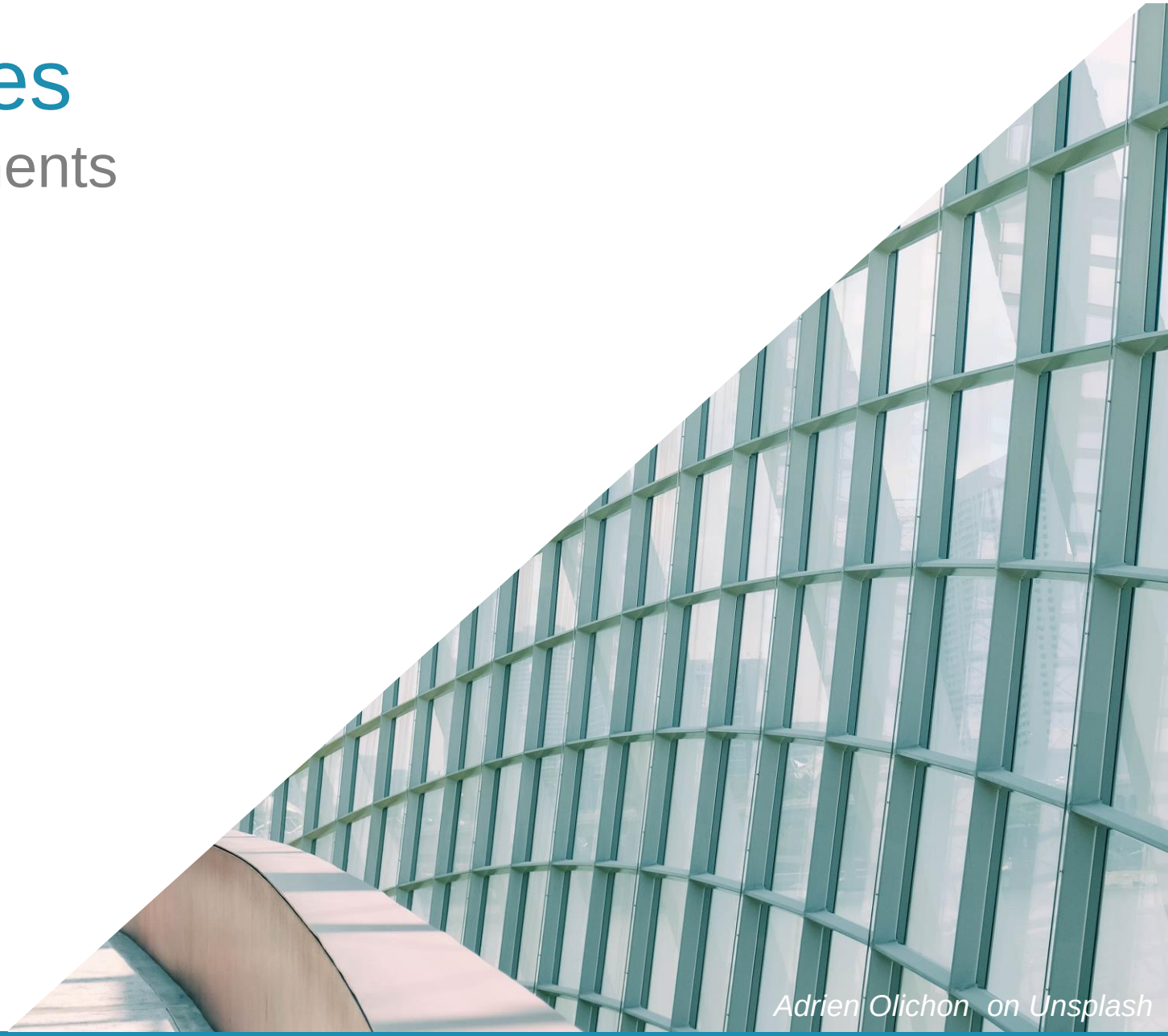
- Cybersecurity Act Certification Schemes (voluntary, unless specified by UE or MS law)

Issue

Diverging mechanisms in the internal market

Rec.

Enhance trans-national cooperation on security, avoiding duplication



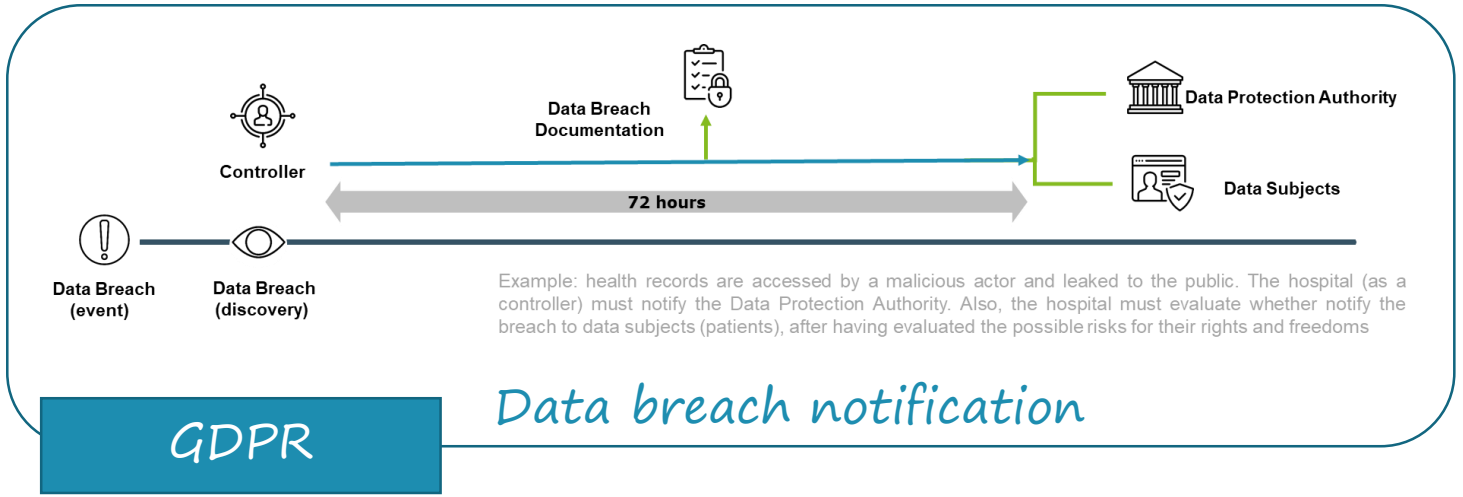
Adrien Olichon on Unsplash

Regulatory challenges

Horizontal and vertical consistency

Duplication (on *Multi-level regulation*, see Choudhoury et al, 2012)

Requirements



- Duplication of tasks
- (Costs for companies)
- 'Risks of contradiction between regulators
- 'Functional underlap'

(Rommel et al, 2010; Hood, 2001)

Issue

Ethical concerns beyond the legal framework

Sections

1. Introduction (principlism and moral principles)
2. Breach of privacy conflict with the principle of justice
3. Breach of safety conflicts with principle of non-maleficence
4. Responsibility allocation


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Ethical concerns beyond the legal framework

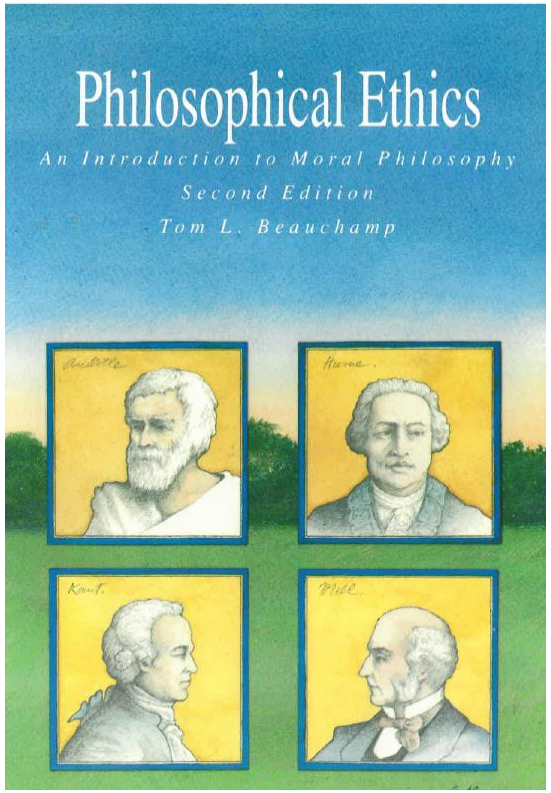
Introduction (principlism and moral principles)

Principlism as a starting point for ethical analysis

Beauchamp & Childress

Principles of Biomedical Ethics (1977; 2009)

- Respect for autonomy
- Non-maleficence
- Beneficence
- Justice

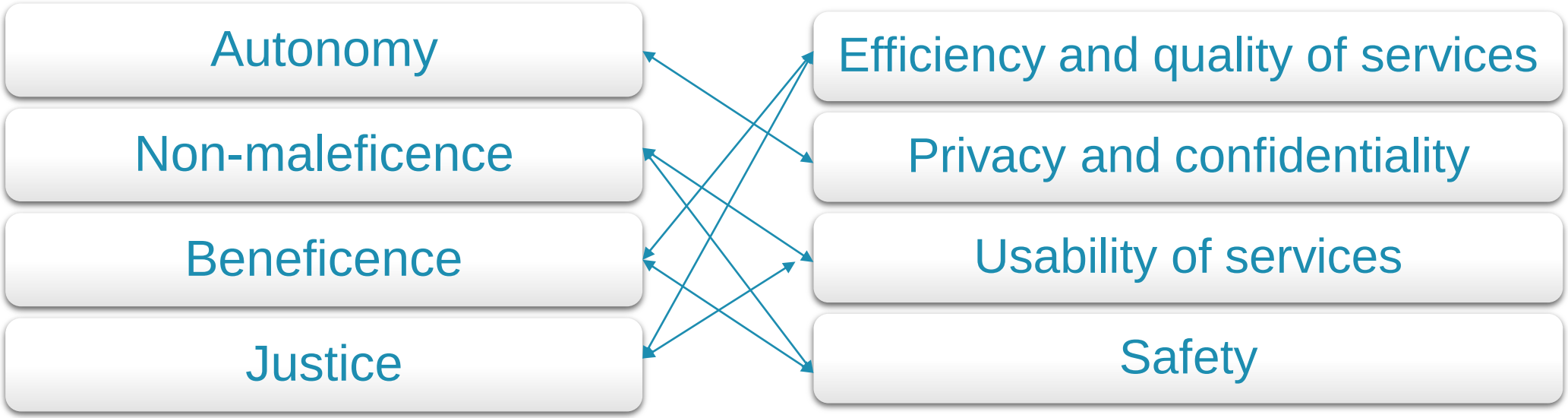


(Beauchamp & Childress 2009; cfr. Danner Clouser & Gert 1990)

Ethical concerns beyond the legal framework

Introduction (principlism and moral principles)

Technical aims mapping to ethical principles



(Loi et al 2020; Weber & Kleine, 2020; SAFECARE D3.9, 2019)

Ethical concerns beyond the legal framework

Breach of privacy conflicts with the principle of justice

In the medical context, **privacy is pivotal for safeguarding patients' autonomy** and reducing their status of vulnerability.

A security incident on a medical device may

- impact **duty of medical confidentiality**
- could lead to destruction, loss, alteration, or unauthorized disclosure of personal data. The misuse of data could cause **unjust discrimination or stigmatization** of the patient *(>< justice*)
- **Undermine trust** towards
  - healthcare practitioners
  - reliability of healthcare system

  (Vedder et al, 2012 and 2014)

Ethical concerns beyond the legal frameworks

Breach of safety conflicts with principle of non-maleficence

Examples: (general)

- destruction, loss, alteration, or unauthorized access or disclosure of data
- Malware spread
- Device manipulation

(Black Hat 2011)

Example: (Brain-Computer Interface)

- Losing special mobility
- Losing control of a given device (wheelchair)

(Ienca et al, 2016)

Ethical concerns beyond the legal frameworks

Responsibility allocation

How to allocate responsibility when a security incident occurs?

- **Variety of stakeholders**
  - (healthcare providers, healthcare professional, patient, manufacturer, network provider)

- Allocation of **(moral) responsibility**
  - *Quid de* liability allocation?
    - Plethora of legal domains
    - (–> ‘Cybersecurity as a joint responsibility’)

(Gerke et al, 2019)

2427999 *on Pixabay*

Other examples

Retrieved from the MDCG Guidance

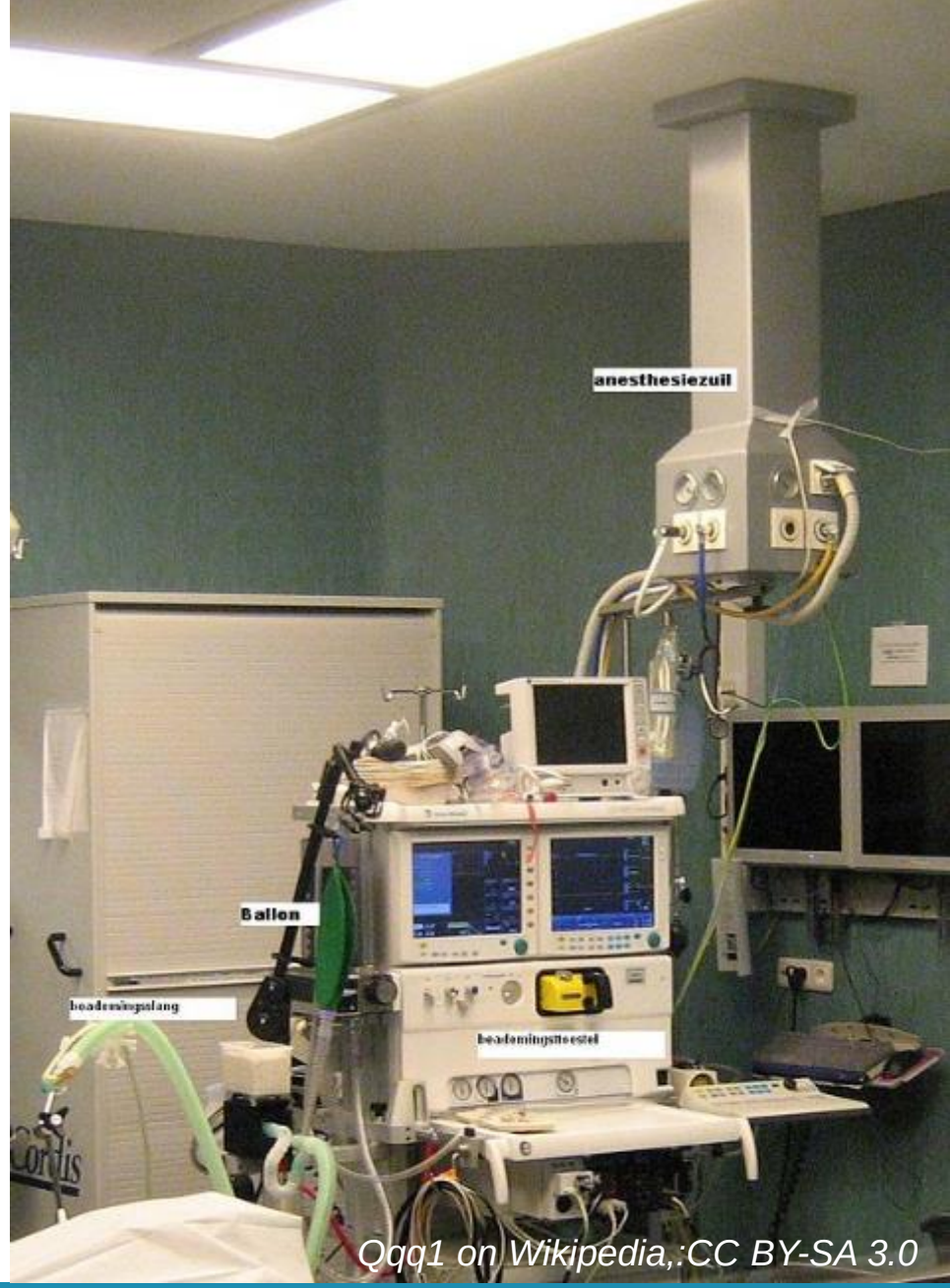
Serious incident	Yes
Risk Relationship	Security risk with a safety impact.
Device	**Anaesthesia device**
Security Harm	An unauthorized user with physical access to the device guesses the weak password for the service account and manipulates the configuration settings.
Safety harm	The anaesthesia device **supplies a wrong anesthetic concentration**

DiverDave on Wikipedia,:CC BY-SA 3.0

Other examples

Retrieved from the MDCG Guidance

Serious incident	Yes
Risk Relationship	Security risk with a safety impact.
Device	**Ventilator**
Security Harm	An attacker with physical access installs malware on the device via the USB interface.
Safety harm	**The respiration functionality of the device does not work as intended.**

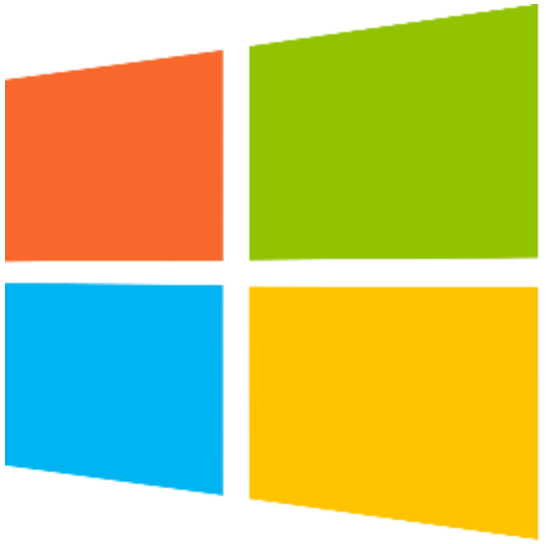


Qqq1 on Wikipedia,:CC BY-SA 3.0

Other examples

Retrieved from the MDCG Guidance

Serious incident	Yes
Risk Relationship	Security risk within indirect safety impact. (device availability)
Device	**Any medical device with Windows**
Security Harm	Network spread malware (worm) encrypts to content of system drive
Safety harm	No direct safety harm. (Indirect: MD not available)



Thank you!

KU Leuven Centre for IT & IP Law (CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

http://www.law.kuleuven.be/citip

imec KU LEUVEN CiTiP CENTRE FOR IT & IP LAW

Annex

Annex

Bibliography

- Biasin, E, Bresic, D, Kamenjasevic, E, Notermans P, (2019) 'SAFECARE D3.9 Analysis of ethics, privacy, and confidentiality constraints' link
- Biasin E., Kamenjasevic, E., (2020) *Should We Think of Contact Tracing Apps As Medical Devices?,* CiTiP Blog link
- Biasin E, Siapka, A., (2020), *SAFECARE D7.2 Training guide for threat response – Legal and Ethical Aspects for Healthcare Cybersecurity*
- Biasin E, (2019) *Medical devices cybersecurity: a growing concern?* CiTiP Blog link
- COCIR, (2019) *Advancing Cybersecurity of Health and Digital Technologies*, link.
- Choudhoury N, Wessel, R., (2012) *Conceptualising Multilevel Regulation in the EU: A Legal Translation of Multilevel Governance?* In European Law Journal, Vol 18 (3), 335
- Danner Clouser, D., Gert, B., (1990) A *Critique of Principlism* in The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine 15(2), 219

Annex

Bibliography

- Fuster, G. G., Jasmontaite, L., (2020) *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights,* in *The Ethics of Cybersecurity* (Christen M. et al eds) Springer link
- Gerke, S. et al., (2019) Ethical and legal issues of ingestible electronic sensors Nature Elect ronics (2), 329
- Ienca, M., Haselager, P, (2016) *Hacking the brain: brain-computer interfacing technology,* in Ethics Inf Tech
- Kasper, A., Antonov A., (2019) *Towards Conceptualizing EU Cybersecurity Law,* Discussion Paper, link
- Kamenjasevic, E. Biasin, E, '*What about viruses doctors cannot treat?" Medical devices, cybersecurity and a duty to provide cyber-trainings* Transformative Technologies: Legal and Ethical Challenges of XXI Century International Conference Co-organised by The European Division of the UNESCO Chair in Bioethics; The Center for the Study of Bioethics; The Law Faculty for the Study of Bioethics
- Kamenjasevic, E., Biasin, E., 2020, *Does EU Medical Devices Directive Apply to Contact Proximity Tracing Apps?* (European Pharmaceutical Law Review link
- Loi, M. et al., 2019, *Cybersecurity in health – disentangling value tensions* in Journal of Information, Communication and Ethics in Society Vol. 17 No. 2, 2019, 229

Annex

Bibliography

- Minssen, T., et al, (2020) *When does stand-alone software qualify as a medical device in the European union?—The CJEU's decision in Snitem and what it implies for the next generation of medical devices,* in Medical Law Review, Vol. 0, No. 0, pp. 1–10 link
- Rommel J. et al, (2010) *Specialization and Fragmentation in Regulatory Regimes, in* Governance of Public Sector Organizations. Governance and Public Management (in In: Lægreid P., Verhoest K. (eds) Palgrave Macmillan,
- Schatz, D. et al, (2017) *Towards a More Representative Definition of Cyber Security*, Journal of Digital Forensics, Security and Law: Vol. 12 : No. 2 , Article 8. link
- Vedder A. et al, (2012) *Trust and e-Healthcare: a Conceptual and Legal Analysis*, Tilburg: TILT
- Vedder A. et al, (2014) *The Law as 'Catalyst and Facilitator' for Trust in E-Health: Challenges and Opportunities, in* Law, Innovation and Technology
- Vedder, A., (2019) *Safety, Security and Ethics*, in Security and Law (Anton Vedder et al. eds.) Intersentia

Annex

Bibliography

- Yaghmaei E. et al, 2019, CANVAS *White Paper 1 – Cybersecurity and Ethics*
- Weber, K., Kleine N., (2020) *Cybersecurity in Health Care, in The Ethics of Cybersecurity* (Christen M. et al eds) Springer
- Wessel R.A., (2015) *Towards EU cybersecurity law: regulating a new policy field*, in Research handbook on international law and cyberspace (Tsagourias N & Buchan R eds) Edward Elgar Publishing

Funding acknowledgement

SAFECARE has received funding as part of the "Secure societies Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002