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
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
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

**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.
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).
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.
Cybersecurity of medical devices: legal and ethical challenges

Biasin, E., Kamenjasevic, E.

- 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.
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
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)

“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

Source: Fuster & Jasmontaite, in The ethics of cybersecurity, CC BY 4.0
Regulatory challenges
Cybersecurity and its conceptualisation

**Security-by-design**
(Recital 12 CSA)

**Security-by-default**
(Recital 13 CSA)

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

*Joint McGuffin*
Cybersecurity of medical devices: legal and ethical challenges

Biasin, E., Kamenjasevic, E.

Regulatory challenges
Consistency requirements

- **Horizontal Consistency**
  - Different policy fields to be combined

- **Vertical Consistency**
  - Measures to be taken both at the national and EU level

- **Both**
  - Different policy fields and different measures at national and EU level

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

- 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))
Regulatory challenges
Horizontal consistency requirements

Uncertainty

- 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)
Regulatory challenges
Vertical consistency requirements

Fragmentation

- 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
Regulatory challenges
Horizontal and vertical consistency

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

- Duplication of tasks
- (Costs for companies)
- ‘Risks of contradiction between regulators
- ‘Functional underlap’ (Rommel et al, 2010; Hood, 2001)

Data breach notification

Example: health records are accessed by a malicious actor and leaked to the public. The hospital (as a controller) must notify the Data Protection Authority. Also, the hospital must evaluate whether notify the breach to data subjects (patients), after having evaluated the possible risks for their rights and freedoms.
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!

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 (UTC time).
Cybersecurity of medical devices: legal and ethical challenges

Biasin, E., Kamenjasevic, E.

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

- Autonomy
- Non-maleficence
- Beneficence
- Justice
- Efficiency and quality of services
- Privacy and confidentiality
- Usability of services
- Safety

(Loi et al 2020; Weber & Kleine, 2020; SAFECARE D3.9, 2019)
Cybersecurity of medical devices: legal and ethical challenges

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

Ethical concerns beyond the legal framework
Breach of privacy conflicts with the principle of justice

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)
### Other examples
Retrieved from the MDCG Guidance

<table>
<thead>
<tr>
<th>Serious incident</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Relationship</td>
<td>Security risk with a safety impact.</td>
</tr>
<tr>
<td>Device</td>
<td>Anaesthesia device</td>
</tr>
<tr>
<td>Security Harm</td>
<td>An unauthorized user with physical access to the device guesses the weak password for the service account and manipulates the configuration settings.</td>
</tr>
<tr>
<td>Safety harm</td>
<td>The anaesthesia device supplies a wrong anesthetic concentration</td>
</tr>
</tbody>
</table>
Other examples  
Retrieved from the MDCG Guidance

<table>
<thead>
<tr>
<th>Serious incident</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Relationship</td>
<td>Security risk with a safety impact.</td>
</tr>
<tr>
<td>Device</td>
<td>Ventilator</td>
</tr>
<tr>
<td>Security Harm</td>
<td>An attacker with physical access installs malware on the device via the USB interface.</td>
</tr>
<tr>
<td>Safety harm</td>
<td>The respiration functionality of the device does not work as intended.</td>
</tr>
</tbody>
</table>
**Other examples**
Retrieved from the MDCG Guidance

<table>
<thead>
<tr>
<th>Serious incident</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Relationship</td>
<td>Security risk within indirect safety impact. (device availability)</td>
</tr>
<tr>
<td>Device</td>
<td><strong>Any medical device with Windows</strong></td>
</tr>
<tr>
<td>Security Harm</td>
<td>Network spread malware (worm) encrypts to content of system drive</td>
</tr>
<tr>
<td>Safety harm</td>
<td>No direct safety harm. (Indirect: MD not available)</td>
</tr>
</tbody>
</table>
Annex
Annex

Bibliography

- Biasin E., Kamenjasevic, E., (2020) Should We Think of Contact Tracing Apps As Medical Devices?, CiTiP Blog link
Annex

Bibliography

- 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
Annex

Bibliography


Annex

Bibliography

- Yaghmaei E. et al, 2019, CANVAS White Paper 1 – Cybersecurity and Ethics

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

These slides are released under the following Creative Commons Licence: Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)