European Health Law & Technology

Università di Pisa

With the support of the Erasmus+ programme of the european union

Open-Source Medical Devices: a Pathway to Safe Medical Technologies

Maria Elena Lippi, PhD candidate in Comparative Private Law at the University of Pisa

OSMDs: a Brief Introduction

OS = not a novelty (a long story of “open philosophy”)

OS software → “software with accessible source code” (Debian Free Software Guidelines) – Software in MD and software as MD

OS hardware → “hardware whose design is made publicly available so that anyone can study, modify, distribute, make, and sell the design or hardware based on that design” (Open-Source Hardware Association).

Improving Accessibility, Safety and Sustainability

- Shares of codes and information (**open innovation**).
- Creation of communities
- Individuation and solution of specific problems (e.g., territorial issues)
- Reachability of remote and disadvantaged communities
- Increase in **safety and security** (Linus' law)
- Reduction of monetary costs.

Health for Society at Large

Open innovation → fair innovation

A benefit for:

- disadvantaged countries
- disadvantaged groups both in high income countries and low/middle income countries (O'Cathaoir)

Safety First!

WARNING: compliance with legally binding standards.

A safe device: “a device that will keep us free from harm” (Nemeth, 2011).

- What kind of harms? Physical damages? Informational damages

Is openness a suitable paradigm for safety in healthcare? How faster is the response to safety issues in OS compared to proprietary software-driven medical devices?

Safety and Security

- Processing of (sensitive) personal information: **data protection law** comes to the fore (a fundamental right)

E.g., the EU GDPR notion of "personal data" and of "personal data processing" is extremely broad - Article 4(1) and (2). – GDPR as EU golden standard.

E.g., Chapter IX of the MDR 2017/745:
- Article 110 (Data Protection)

- Does OS constitute another layer of risk?

Article 4, GDPR

1.‘**Personal data**’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2.‘**Processing**’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

DPL principles

Article 5, GDPR: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.

Article 9, GDPR → reinforced protection to "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

Article 7, GDPR → principle of consent

Article 25, GDPR → privacy by design and by default

Article 32, GDPR → security

Article 32, GDPR

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk"

E.g., pseudonymisation and encryption; ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services; restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident; regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

DPL challenges

- Where are data stored (online/offline)? Is medical device personalised? Are there any apps related to the device?
- How to assess the roles defined by the GDPR?
- In the everchanging environment of OS, how to respect principles such as privacy by default and privacy by design? How to deal with data minimization?
- Can OS become an organizational measure against security threats (Article 32, GDPR)?

DPL and OSMDs

- Comparison with proprietary software: at present, there is no clear evidence to prefer proprietary software over OS in terms of prevention of data breaches.

- Decentralisation as a suitable organizational measure to control possible threats - E.g., enhancing of reliability: «Only algorithms and implementations that have been thoroughly peer-reviewed can possibly be trusted as secure» (Raymond)

- Prevention and an ex post solution to fix vulnerabilities.

OS software «can have significantly better resilience to unexpected input than their proprietary counterparts» (Boulanger).

DPL and OSMDs

- In light of the GDPR's principles: granting data security even for disadvantaged areas and social groups

E.g., «while European countries have built a strong foundation for data security, with the entry into force of the GDPR, more lax standards are often in place in the Global South […] there is a risk of data misuses to benefit the wealthy, without ensuring access for the vulnerable» (O'Cathaoir)

The role of IPL

- **Intellectual property law** impacts on software and hardware development and commerciability.

- Software components: «Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971)» (art. 10.1, TRIPs Agreement) – forms of expression; algorithms can be protected as trade secrets.
- Hardware components: e.g., patents registration system.
- Databases: sui generis right (EU)

OS does NOT imply a complete refusal of copyright

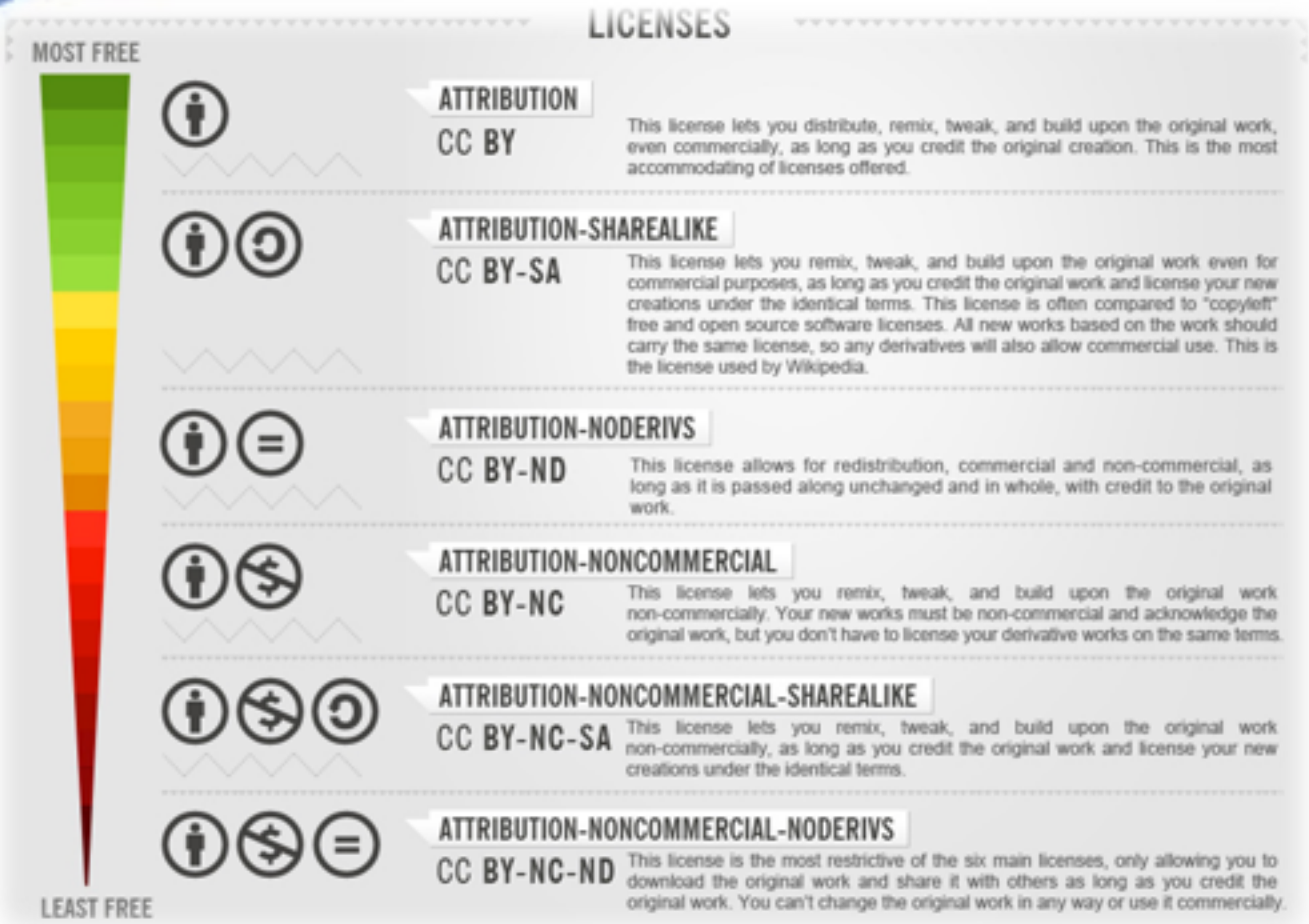
The role of IPL

IP centralization vs OS decentralization

- IPL creates scarcity and barriers to competition.
- Public domain implies benefitting the public interest
- Different incentives (e.g., reputation, prestige, "the joy of programming"; humanitarian afflatus)

E.g., the case of prosthesis: «the IP owner could **forbid** the use of a prosthesis without their permission even if the MD regime, the prosthetic user, and the clinical team would like this to be done» (Brown et al.)

Creative Commons



Organisation

Do not forget: OSMDs are made by a combination of technical aspects and human resources.

Transparency and **expertise** → OS communities should rely on some forms of hierarchies and clear organisation (the importance of mentors in OS projects).

OSMDs' goals

- Improving clarity and an effective self-surveillance (e.g., avoiding hazards through real share of information and documentation in the OS communities).
- Involving users in the various phases of the device development (reliability).
- **Regulation by design**: careful compliance with standards (see the UBORA model).
- Aiming at a general and legally consistent definition of OSMDs.

Some example from the EU:

- Open source software strategy | European Commission (europa.eu), in which the concept of ‘OS’ has been linked to the concept of ‘public service’.

- EU-FOSSA 2 - Free and Open Source Software Auditing | European Commission (europa.eu) → «**bug bounties**, which **reward people** for finding and reporting vulnerabilities existing in free and open source software, are one of the main activities of the EU-FOSSA project. Three bug bounty platforms were selected to organise the hunt for bugs in several critical free and open source software packages used by European institutions.»

Thank you for your attention!

website at

Scan Me

https://twitter.com/ELaTeUnipi

mail at elate@jus.unipi.it

https://elate.jus.unipi.it/