Security and Privacy by Design for Healthcare

New solutions from EU H2020 Projects to comply with GDPR, Medical Device Regulation, EU Directive 2016/1148 on essential services and COVID context

Insights and recommendations from research and innovations projects and entities

2021

Acknowledgements

Cyberwatching.eu is grateful to the projects and individual experts that have contributed to the series of webinars of the project clusters on the topic of security and privacy by design in the healthcare sector, and to the recommendations provided in this document. More details and contact details can be found in section 5.

Disclaimer

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under Grant Agreement no.740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Contents

1 Introduction 4
2 Security and Privacy-by-Design for Healthcare 5
2.1 Challenges and an overview of the proposed solutions 5
2.2 The Roadmap to GDPR Compliance in e-Healthcare Services 8
3 Insights and recommendations from R&I projects 11
3.1 DEFeND: Data Governance for Supporting GDPR 11
3.2 PANACEA: Protection and priVacy of hospital and health iNfrastructures with smart Cyber sEcurity and cyber threat toolkit for dAta and people 12
3.3 PAPAYA: PlAtform for PrivAcY preserving data Analytics 15
4 Conclusion 16
5 Contributing projects and entities 17
How to reach us 18

List of Figures

Figure 1. An overview of how DEFeND, PANACEA and PAPAYA solutions may help you 8
Figure 2. Applicable Legal Framework for the Health sector 9

1 Introduction

Cyberwatching.eu aims to improve the impact of the results of research and innovation projects in the European Union and Associated Countries, and to achieve this, the overall cyberwatching.eu methodology is founded on the following 3 macro activities: 1) Clustering & synergising; 2) Engaging; 3) Supporting. Each macro-activity, at an operational level, translates effectively into a series of tasks, executed utilising some specific tools and levers. Detailed information about this process can be read in the D2.3 Methodology for Classification and Marker Readiness[1].

As a follow-up of the virtual meetings[2] held last July 2020, Cyberwatching.eu has supported collaboration and mini-clusters[3] between R&I projects focusing on cybersecurity solutions and best practices in vertical sectors and horizontal topics.

- Healthcare[4]
- Energy[5]
- Finance[6]
- Critical infrastructure[7]
- Threat Intelligence[8]
- GDPR[9]

The topic of this joint webinar was **security and privacy by design for the healthcare sector[10].** Three projects presenting their solutions: DEFEND[11], PANACEA[12] and PAPAYA[13]. The webinar also showed the strength and depth of work being carried out by these R&I projects in providing solutions that have security and privacy by design at the very core of them. At a time when health systems are at full-stretch to deal with the current COVID-19 pandemic, and researchers are collaborating together to create and provide new vaccines, the webinar demonstrated the value of alignment and collaboration between R&I projects in the field of cybersecurity and privacy to support health organisations and manufacturers of medical devices to be able to provide resilient and trusted services.

[1] https://cyberwatching.eu/d23-methodology-classification-projectsservices-and-market-readiness
[2] https://www.cyberwatching.eu/news-events/news/boosting-synergies-improve-market-readiness-levels-projects
[3] https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters
[4] https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters/health
[5] https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters/energy
[6] https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters/finance
[7] https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters/critical-infrastructure
[8] https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters/threat-intelligence
[9] https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters/gdpr
[10] https://cyberwatching.eu/security-and-privacy-design-healthcare
[11] https://cyberwatching.eu/projects/1039/defend
[12] https://cyberwatching.eu/projects/1270/panacea
[13] https://cyberwatching.eu/projects/974/papaya

2 Security and Privacy-by-Design for Healthcare

Delivery of health services (clinical and administrative) through ICT and connected medical devices is a necessity for healthcare organisations and changes the way healthcare services are delivered and data are shared. Therefore, cyberattacks and staff misbehaviour may have significant negative effects on business continuity, patients' safety and data privacy.

Current levels of privacy protection and security are highly dependent on the intrinsic risk embedded in the existing systems, medical devices and procedures: in a long-term perspective, if the investments for physiological renewal/upgrade of these assets were inspired by a "privacy and security by design" approach, the overall risk would decrease.

In accordance with this approach, the European Commission has set up regulatory measures (e.g., GDPR, MDR, EU Directive 2016/1148), and also, through the Horizon 2020 programme, funded research and innovation projects to develop solutions that are effective and usable in the healthcare context to reduce the overall ex-ante risk. This includes threats specific to COVID-like situations.

This joint webinar was organised by Cyberwatching.eu following its aim to cluster active projects with similar goals for their mutual benefit, by identifying possible opportunities for lightweight synergies and supporting them with targeted support activities. The webinar took place on 10 December 2020 at 11 AM CET in collaboration with the DEFeND, PANACEA and PAPAYA projects.

With representatives from the health, legal and cybersecurity sectors, this webinar presented the main challenges facing the medical sector in ensuring secure integration of services that comply with EU regulations, and the three cutting-edge security and privacy-by-design solutions under development thanks to EC-funding.

2.1 Challenges and an overview of the proposed solutions

Gemelli
Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

Website: www.policlinicogemelli.it
Contributor: Sabina Magalini[14]
Senior Surgeon of the Emergency and Trauma Surgery Unit at the Fondazione Policlinico Universitario Gemelli (FPG)

Dr Sabina Magalini highlighted the urgent need for security and privacy-by-design solutions in healthcare given the following challenges that we are facing such as:

- **Hospitals and digital service providers need «protocols» for secure integration**
  - Systems developers and medical device manufacturers need to apply security and privacy by design approaches.

[14] https://cyberwatching.eu/sabina-magalini

- Also, hospitals and digital service providers need to master security and privacy by design, when they procure and deploy the assets.

- **All healthcare actors need to comply with the EU regulatory framework**

  - **GDPR (EU) 2016/679**

    Art.25 Data protection by *design and by default: ... the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, … designed to implement data-protection principles.*

    Art.30 Records of processing activities: … Each controller … shall maintain a record of processing activities under its responsibility…Each processor ... shall maintain a record of all categories of processing activities carried out

  - **Directive (EU) 2016/1148 (NIS) concerning measures for a high common level of security of network and information systems across the Union.**

    Whereas 50): … manufacturers and software developers … play an important role in enabling operators of essential services and digital service providers to secure their network and information systems.

  - **Medical Devise Regulation (EU) 2017/745**

    Requirements regarding design and manufacture. 17.2: For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of the development life cycle, risk management, including information security, verification and validation.

  - **Cyber Regulation (EU) 2019/881**

    Reinforce by the said regulation, which establishes an EU-wide cybersecurity certification framework for digital products, services and processes.

- **COVID-like context raises specific requirements, pointing to security and privacy by design**

  - **Telemedicine**: the policy to keep non-severe COVID patients at home plus the need for telemonitoring, expanding the use of telemedicine, which has a low level of security.

  - **Smart working**: Risk may come from technology illiteracy of the staff at home and increased risk of infection due to connections from potentially defenceless home devices; carelessness in exchanging credentials with colleagues to VPN or shared folders.

  - **Use of new staff**: newly hired healthcare personnel have inexperience of company cybersecurity and privacy policies, sudden arrival of massive new staff can weaken the provisioning, de-provisioning and profiling processes, leading to security issues.

  - **Need for ad-hoc IT solutions fast design**: the healthcare sector needs to rapidly design and

deploy apps and back-end systems. Fast design risk delivering non-secure solutions.

- **Infection monitoring data flow**: there has been a major demand for data flux to monitor infections, to do epidemiological reporting, etc. These data fluxes take place between many institutions; information sharing has a low level of security.

- **Non-healthcare sites used for healthcare operations**: temporary hospitals, churches, nearby hotels, other empty but usable spaces have been upgraded to "hospital-level". WIFI systems of these structures, in general, are not secure. Hackers can monitor traffic over the air to steal access credentials.

Over the last few years, ICT and connected medical devices have become mission-critical for healthcare operations, but still, poorly protected and vulnerable. Therefore, cyberattacks and incorrect staff behaviour are growing risks for business continuity, patients' safety and data privacy.

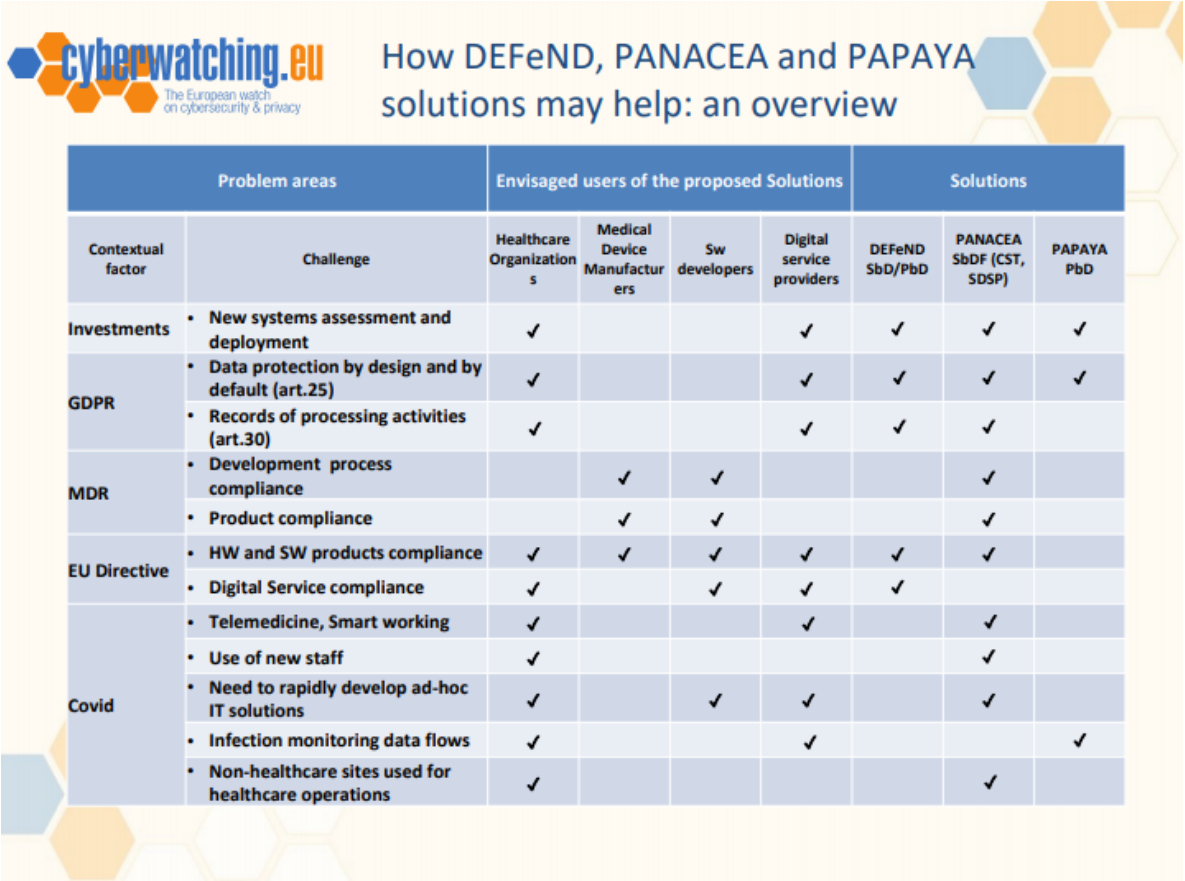
The **current level of privacy protection and security must be improved**, also because most of the existing assets were designed when data privacy and cybersecurity were not an issue.

This COVID era offers the opportunity to renew the systems. A way to radically improve is to invest, to substitute/upgrade "obsolete" assets, adopting a "security and privacy by design" approach. A positive side-effect of COVID-19 in Europe is that it has brought to the surface the weaknesses of the national health services and the needs to invest in e-health and telehealth, with the European recovery funds. The new investment will somehow upgrade the system as e-health and telehealth are the future.

The European Commission (EC) response to the need for security and privacy by design includes not only the revamping and strengthening of ENISA[15] (the EU Agency for cybersecurity, through Cyber Act 2019/881) and regulatory measures (GDPR, MDR, EU Directive 2016/1148, Cyber Act 2019/881) but also the funding, through the Horizon 2020 programme, of research and innovation projects to develop solutions that are effective and usable in the healthcare context. DEFeND, PANACEA and PAPAYA are three of them.

The three projects collaborated to design a table as shown in figure 1 that can be very useful to understand how these projects have developed solutions that can help to tackle problem areas and specific challenges relative to the healthcare sector.

[15] https://www.enisa.europa.eu/



Problem areas		Envisaged users of the proposed Solutions				Solutions		
Contextual factor	Challenge	Healthcare Organizations	Medical Device Manufacturers	Sw developers	Digital service providers	DEFeND SbD/PbD	PANACEA SbDF (CST, SDSP)	PAPAYA PbD
Investments	• New systems assessment and deployment	✓			✓	✓	✓	✓
GDPR	• Data protection by design and by default (art.25)	✓			✓	✓	✓	✓
	• Records of processing activities (art.30)	✓			✓	✓	✓	
MDR	• Development process compliance		✓	✓			✓	
	• Product compliance		✓	✓			✓	
EU Directive	• HW and SW products compliance	✓	✓	✓	✓	✓	✓	
	• Digital Service compliance	✓		✓	✓	✓		
Covid	• Telemedicine, Smart working	✓			✓		✓	
	• Use of new staff	✓					✓	
	• Need to rapidly develop ad-hoc IT solutions	✓		✓	✓		✓	
	• Infection monitoring data flows	✓			✓			✓
	• Non-healthcare sites used for healthcare operations	✓					✓	

Figure 1. An overview of how DEFeND, PANACEA and PAPAYA solutions may help you

2.2 The Roadmap to GDPR Compliance in e-Healthcare Services

Website: www.ictlegalconsulting.com
Contributor: Anastasia Botsi[16]
Associate at ICT Legal Consulting

The COVID-19 situation is a wake-up call to all the actors involved in the sector. Especially from a GDPR perspective, organisations need to start taking this issue more seriously and seeing this regulation not just as a requirement that is there to make their life difficult but a useful tool that can help and assist in ensuring a safer environment, and is more privacy-friendly for the patients, doctors and all that are involved.

Anastasia Botsi, representing the legal partner of the Cyberwatching.eu project, provided an

[16] https://cyberwatching.eu/anastasia-botsi

overview of the roadmap to comply with the General Data Protection Regulation (GDPR)[17] in healthcare services taking into account the legal framework applicable for healthcare services.

There are three main legal frameworks and regulations applicable in the context of the health sector.

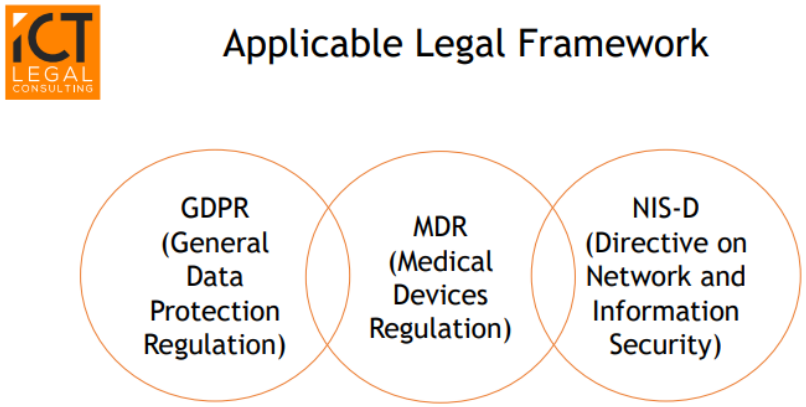


Figure 2. Applicable Legal Framework for the Health sector

- **GDPR – General Data Protection Regulation**

  Indicates principles and obligations relating to the protection of rights and freedoms of data subjects, e.g., data protection by design and by default, and principles of lawfulness, fairness and transparency, and data protection impact assessments, and security measures.

  - **Special categories of personal data:** data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.
  - **Data concerning health** means personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
  - **Genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
  - **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.

- **MDR – Medical Devices Regulation**

  Ensure a consistently high level of health and safety protection for EU citizens using medical devices:

  - Defining devices in the healthcare sector and classifying them

[17] https://cyberwatching.eu/policy-landscape/privacy/general-data-protection-regulation

- Designing and manufacturing medical devices
- Making available or putting into service medical devices for human use and placing them on the market.

- **NIS-D – Directive on Network and Information Security**

  Establishes a common level of security for network and information systems focusing on Essential Service Providers and Digital Service Providers, e.g., security requirements, and incident notifications and coordination of computer incident response teams.

The ICT Legal presentation has introduced the Information Notice Tool[18], which was developed as part of the Cyberwatching.eu initiative for informative and awareness purposes, mainly focussed on assisting H2020 Projects and SMEs in evaluating their privacy policies and amending them based on the obligatory components of Articles 13 and 14.

This tool consists of questions about the data processing activities, also providing corresponding recommendations coming directly from ICT Legal Consulting, a law firm with plenty of expertise in the area.

Any organisation that processes personal data must ensure that data subjects are informed about their rights and how to freely exercise them:

- Right of access (Art. 15 GDPR): by what means the persons concerned can obtain the information relating to them.
- Right to rectification (Art. 16 GDPR): how to complete incomplete/inaccurate data.
- Right to erasure (Art. 17 GDPR): allowing the deletion of any data relating to the data subject.
- Right to restrict processing (Art. 18 GDPR): under certain conditions, the data subject may request for the organisation to restrict its processing.

Council of Europe Recommendation on the protection of health-related data

Here are a set of principles to protect health-related data, including:

- "Personal data protection principles should be taken into account by default (privacy by default) and incorporated right from the design of information systems, which process health-related data (privacy by design). Compliance with these principles should be regularly reviewed throughout the life cycle of the processing. The controller should carry out, before commencing the processing and at regular intervals, an assessment of the potential impact of the foreseen processing of data in terms of data protection and respect for privacy, including of the measures aimed at mitigating the risk." [Recommendation 4.2].
- Protecting health-related data flows "Transborder data flows may only take place where an appropriate level of data protection is secured in accordance with the safeguards provided for in Convention 108" [Recommendation 17].

[18] https://cyberwatching.eu/cyberwatching-information-notice-tool

3 Insights and recommendations from R&I projects

3.1 DEFeND: Data Governance for Supporting GDPR

Website: www.defendproject.eu
Duration: July 2018 – March 2021
Contributor:
Andrés Castillo[19], Pediatric Hospital Niño Jesús, and Haris Mouratidis[20], University of Brighton

DEFeND presented its innovative data privacy governance platform reporting the main project objectives:

- Design and development of a successful **market-oriented, platform** to support organizations towards GDPR compliance
- Develop a **modular solution** that covers different aspects of the GDPR
- **Automated** methods and techniques to elicit, map and **analyse data** that organizations hold for individuals
- Advanced modelling languages and methodologies for privacy-by-design and **data protection** management
- Specification, management and enforcement of **personal data consent**
- Integrated **encryption and anonymisation** solutions for GDPR
- **Deployment and validation** of the DEFeND platform in real operations.

Among the main Healthcare and Technical challenges, DEFeND is tackling:

- Redesign hospital data paths according to privacy by design principles;
- Tracking of changes and cancellation of consents;
- Management of health data for research;
- Sharing of health data with other hospitals inside and outside the EU (travellers, tourists, derivations);
- Getting health data from sensors and wearables from patients at home into the hospital (telemedicine contexts);
- Transferring of health data to and from third parties to the hospital (e.g., labs, Insurance);
- Connecting in-hospital emergency department with Emergency Medical Services (e.g., ambulances carrying COVID-19 patients and Multiple Casualties Incidents victims);
- Transforming privacy (social and legal concept, deliberately vague, contextual and subjective) into a technical requirement;
- Deriving technical requirements from GDPR;
- Dealing with conflicts between privacy and security areas;
- Building systems that can support continuous GDPR compliance.

[19] https://cyberwatching.eu/andrés-castillo
[20] https://cyberwatching.eu/haris-mouratidis

Recommendations from DEFeND

- **Ensure continuous GDPR compliance**. GDPR compliance mustn't be seen as a one-off but as a continuous effort. In supporting such an approach, privacy-by-design conceptual languages must be developed that consider the context of an organisation and focus on the relationship between privacy requirements, threats/vulnerabilities and privacy-enhancing technologies. DEFeND has developed the SecTro language to support the foundations of such an approach.

- **Embed a culture of privacy governance.** Privacy mustn't be just considered a burden or a regulatory "have-to" but as an aspect that can benefit the whole organisation. Tools, methods and techniques must be developed to embed privacy governance as part of the organisational culture.

- **Go beyond just technical and legal treatment of privacy**. Solutions should follow a holistic socio-technical approach to the management of privacy, supported by common languages across different sectors (e.g., legal, technical, social, ethical) and different domains (e.g., health, public admin, energy). Such treatment of privacy will improve the efficiency and efficacy of organisational and privacy operations, supports financial impact analysis while operating within an ethical framework.

- **Improve decision-making capabilities**. It is important to improve intelligence and predictive capabilities concerning privacy through technological advancements in areas such as artificial intelligence to enable faster response and resolution of privacy concerns.

3.2 PANACEA: Protection and priVacy of hospital and health iNfrastructures with smart Cyber sEcurity and cyber threat toolkit for dAta and people

Panacea
People-centric cybersecurity in healthcare

Website: www.panacearesearch.eu
Duration: January 2019 – December 2021
Contributor: Martina Bossini Baroggi[21], RINA

Security issues in the healthcare sector start with fragmentation and lack of privacy and cyber awareness. A programmatic approach to the identification, mitigation, and remediation of risk should be developed and implemented at the initial design phase of medical devices, as it is fundamental to introduce right away security aspects, which takes into account cyber risks.

In order to overcome the design limitations of medical devices or systems that include security engineering aspects regarding cyber risks poorly, PANACEA proposes the Security by Design Framework. The main concept is to make systems as free of vulnerabilities and impervious to

[21] https://cyberwatching.eu/martina-bossini-baroggi

attacks as possible through different cybersecurity measures that should be integrated into the design process so that the devices will be designed securely from the foundations.

The approach that has been followed was defined taking into consideration ENISA analysis on potential candidates of cybersecurity certification schemes and could be summarized in five steps:

- Context definition
- Relevant standards/certification schemes identification
- Standards mapping, gap analysis and extraction
- Conformity assessment
- Risk assessment

The domain targeted is the healthcare domain and in particular, the focus is on medical devices and systems design. The device lifecycle has been studied and analysed in order to understand the conformity-related activities for each phase starting from the requirements definition to the deployment and use phase.

After that, an analysis of the key applicable standards was carried out to understand what should be considered during the Medical Device and System Lifecycle. Resulting regulations and standards were: GDPR, MDR/IVDR, ISO 27001, ISO 27799:2008, IEC 80000-1:2010, ISO 13485:2016, ISO14971, IEC 62304:2006.

Some of these standards (ISO 27799, ISO 13485 and ISO 80001-1:2010) are specifically considered in the analysis performed by ENISA (Mapping of EOS Security Requirements to Specific Sectors).

All these standards were analysed and links between them were investigated. For each one of the selected standards, the most relevant articles in terms of cybersecurity were extracted in order to define checklists useful to guide the user to assess conformities. Moreover, from the majority of them, taxonomies such as assets/vulnerabilities/threats/security controls were extracted.

The last two steps are conformity and risk assessment. In PANACEA, the conformity assessment, for which continuous evidence collection and audit are essential, is supported by the **Compliance Support Tool (CST)** and the risk assessment is covered by the **Secure Design Support Platform (SDSP)**.

These two technological solutions compose the PANACEA Security by Design Framework (SbDF). The SbDF was conceived to support medical devices and systems manufacturers for the whole development process to continuously monitor the compliance to standards and at the same time to perform the risk assessment.

CST is designed for internal auditing to support self-awareness on the regulatory side during the development phase, but also for certification auditing as a support to the audit activities. The checklists developed by RINA, extracted by the analysis of several European regulations and in alignment with the ENISA approach, are implemented in CST, which is configured in the Healthcare sector.

SDSP is intended to support the security of a medical device/information system in development, by providing a software platform for risk assessment analysis. Each risk assessment analysis may produce security controls that will lead to new requirements to be embedded in the system in

order to improve its resulting security.

The output of the risk assessment is collected in the CST to cover security controls related to risk management and allows to complete the conformity assessment.

In conclusion, the innovation points and the benefits of these solutions could be highlighted as follows:

- development of tools to support conformity and risk assessment that is fit for the Health Care sector;
- extraction of taxonomies (vulnerabilities/threats/security controls) from health care most relevant standards in order to take into consideration during risk assessments scenarios that are specific for this sector;
- use of the Security-by-design principles to lead the manufacturers in the decision-making of possible security controls to be implemented during software/system engineering early phases
- liaison with ENISA approach and guidelines for the analysis of potential candidates of certification schemes.

Recommendations from PANACEA

- Considering the impact that their widespread adoption may have on cybersecurity, **we recommend inserting a more explicit reference to Security by Design tools in the next version of the "PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS" released by ENISA in February 2020,** specifying that they can be used in the Plan (analyse and collect requirements) and in the Source (prepare a request for proposal tenders, evaluate received proposals) phases of the Procurement Process. ENISA Guidelines have been used by the Security by Design Framework (SbDF) and SDSP specifically as a reference for the configuration of Assets and Health Care domain-specific scenarios. As a consequence, during the PANACEA project, a taxonomy of assets and related scenarios has been introduced into the SDSP platform so that the procurement types described in the ENISA document and these assets are an exact match: from this perspective, the secure design support platform could be evaluated as a practical implementation of ENISA guidelines applied to the risk assessment by design.

- As dealt within PANACEA SbDF and CST specifically, **it is recommended to medical device and application providers but also hospitals and policymakers to sustain continuous monitoring of compliance to information security standards of medical devices/information system along the whole development life-cycle process** in order to trigger faster resolution with security health checks, facilitate auditability, reduce complexity and human errors during the operations and maintenance, therefore decreasing the overburden on organizational processes. By the joint focus on this aspect both from producers and consumers of software/medical devices, it is possible to reduce the gap of regulatory information asymmetry between these actors that cause assurance unclarity and vulnerability;

- Considering that the EC funds many projects (such as PANACEA) that deliver solutions aimed at improving cybersecurity, and considering the need to digitize the Healthcare Sector (after COVID-19) in the context of the Next Generation EU, we **recommend that the EC set up a funding channel to promote the adoption of those solutions (such as tools for Security by Design)**. This

channel could be a co-financing fund that can be used by healthcare organization if they use solutions developed through EU Programmes (such as H2020).

3.3 PAPAYA: PlAtform for PrivAcY preserving data Analytics

Website: www.papaya-project.eu
Duration: May 2018 – April 2021
Contributor: Orhan Ermis[22], EURECOM

The PlAtform for PrivAcY preserving data Analytics (PAPAYA) project is developing privacy-by-design solutions and a dedicated platform for data analytics tasks that are outsourced to untrusted data processors. This will allow stakeholders to ensure their clients' privacy and comply with the European GDPR while extracting valuable and meaningful information from the analysed data.

PAPAYA targets two digital health use cases, namely arrhythmia detection and stress detection, whereby patients' data are protected through dedicated privacy-enhancing technologies.

Recommendations from PAPAYA

The PAPAYA project's recommendations on cybersecurity risk management are as follows:

- The PAPAYA consortium recommends **privacy enhancement technologies (PETs) for making the best possible privacy-utility trade-off in privacy-preserving analytics transparent to data subjects**. Beyond design considerations of analytics PETs, the selection of analytics PETs, their configuration, and parameter selection are central to this trade-off.
- The PAPAYA consortium recommends the **assessment of privacy enhancement technologies (PETs) against a wide range of attacks, considering both passive adversaries (information leakage) and active adversaries.**
- As part of continuous risk management, the PAPAYA consortium recommends that the **data collectors should document threats, their associated determined risk and mitigations**.

[22] https://cyberwatching.eu/orhan-ermis

4 Conclusion

The Cyberwatching.eu webinar on "**Security and Privacy by Design for Healthcare**"[23] provided very useful insights on the main challenges facing the medical sector in ensuring secure integration of services that comply with EU regulations. In order to tackle these challenges, three cutting-edge security and privacy-by-design solutions from Horizon 2020 projects PANACEA, DEFeND and PAPAYA were presented.

The main recommendations from this document are detailed below:

- The **current level of privacy protection and security must be improved**, also because most of the existing assets were designed when data privacy and cybersecurity were not an issue.
- When processing personal data and especially the special categories of personal data, you need to **carefully evaluate the legal basis** that the processing activities involved.
- GDPR compliance mustn't be seen as a one-off but as a continuous effort.
- There's a need to improve the privacy enhancement technologies (PETs) to **make the best possible privacy-utility trade-off in privacy-preserving analytics transparent to data subjects.**
- Next Generation EU and the related recovery plans and investments will be an **opportunity to reduce cyber risk if and only if security and privacy by design approaches are adopted by all involved parties**.
- While waiting for definitive directions on how to implement the cyber act, **hospitals could set up pre-requirements for contracts with medical device manufacturers and system/service providers**. These should state that, in face of similar products, preference is given to those that comply with the security and privacy by design approach.

[23] https://cyberwatching.eu/security-and-privacy-design-healthcare

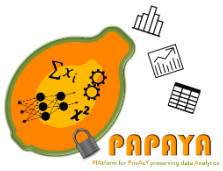
5 Contributing projects and entities

The projects contributing to this document are the following:

Website: www.defendproject.eu
Cyberwatching.eu mini-site:
www.cyberwatching.eu/projects/1039/defend
Cyberatching.eu Grant agreement number: 787068
Duration: 1 July 2018 – 31 March 2021
Contributors:

- Andrés Castillo[24], Pediatric Hospital Niño Jesús
- Haris Mouratidis[25], University of Brighton

Website: www.panacearesearch.eu
Cyberwatching.eu mini-site:
www.cyberwatching.eu/projects/1270/panacea
Grant agreement number: 826293
Duration: 1 January 2019 – 31 December 2021
Contributor: Martina Bossini Baroggi[26], RINA



Website: www.papaya-project.eu
Cyberwatching.eu mini-site:
www.cyberwatching.eu/projects/974/papaya
Grant agreement number: 833955
Duration: 1 May 2018 – 30 April 2021
Contributor: Orhan Ermis[27], EURECOM

Here are participating experts:

Website: www.policlinicogemelli.it
Contributor: Sabina Magalini[28]
Senior Surgeon of the Emergency and Trauma Surgery Unit at the Fondazione Policlinico Universitario Gemelli (FPG)

Website: www.ictlegalconsulting.com
Contributor: Anastasia Botsi[29]
Associate at ICT Legal Consulting

[24] https://cyberwatching.eu/andrés-castillo
[25] https://cyberwatching.eu/haris-mouratidis
[26] https://cyberwatching.eu/martina-bossini-baroggi
[27] https://cyberwatching.eu/orhan-ermis
[28] https://cyberwatching.eu/sabina-magalini
[29] https://cyberwatching.eu/anastasia-botsi

Watch the recorded workshop video now!

You may also download the speakers' presentations on the webinar page.

How to reach us

cyberwatching.eu
The European watch on cybersecurity & privacy

www.cyberwatching.eu

@cyberwatchingeu

in/company/cyberwatchingeu

cyberwatching.eu consortium

Trust-IT Services
Communicating ICT to markets

Oxford e-Research Centre

UNIVERSITY OF OXFORD

ICT LEGAL CONSULTING Balboni Bolognini & Partners

European Digital SME Alliance

CONCEPTIVITY

360 SECURITY

AON

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740129.