ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Eurobank

Secure HealthData

ΑΣΦΑΛΕΙΑ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΥΓΕΙΑ

"Δημόσιο Σύστημα Υγείας, ιατρικά δεδομένα και τα δικαιώματα του πολίτη στην εποχή του GDPR. Προκλήσεις και λύσεις από τη σκοπιά της μηχανοργάνωσης"

Πιτόγλου Σταύρος

CTO Computer Solutions

Computer Solutions
INTEGRATED INFORMATION SYSTEMS

Δημόσιο Σύστημα Υγείας, Ιατρικά Δεδομένα & τα Δικαιώματα του Πολίτη στην Εποχή του GDPR :

Προκλήσεις και Λύσεις από τη Σκοπιά της Μηχανοργάνωσης

MEDINFOBOOK
Medical Information Record

ΕΥΚΑΙΡΙΑ

4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

ΚΙΝΔΥΝΟΣ

4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

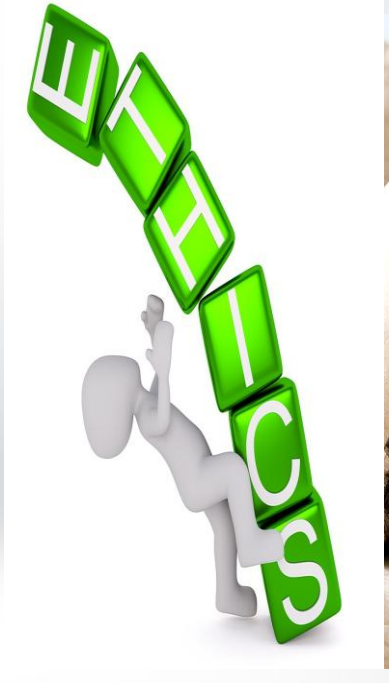
REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

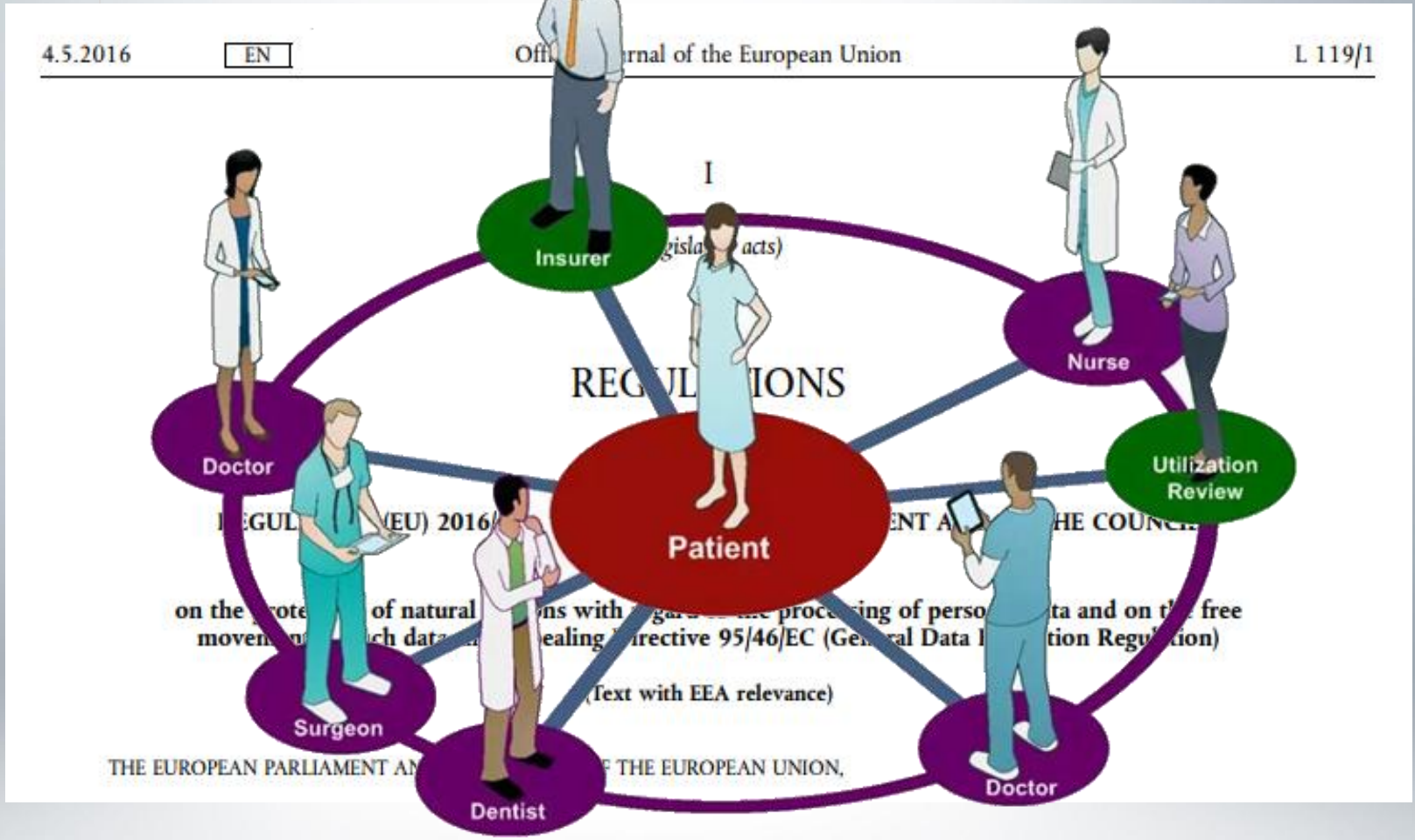
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

ΕΥΚΑΙΡΙΑ

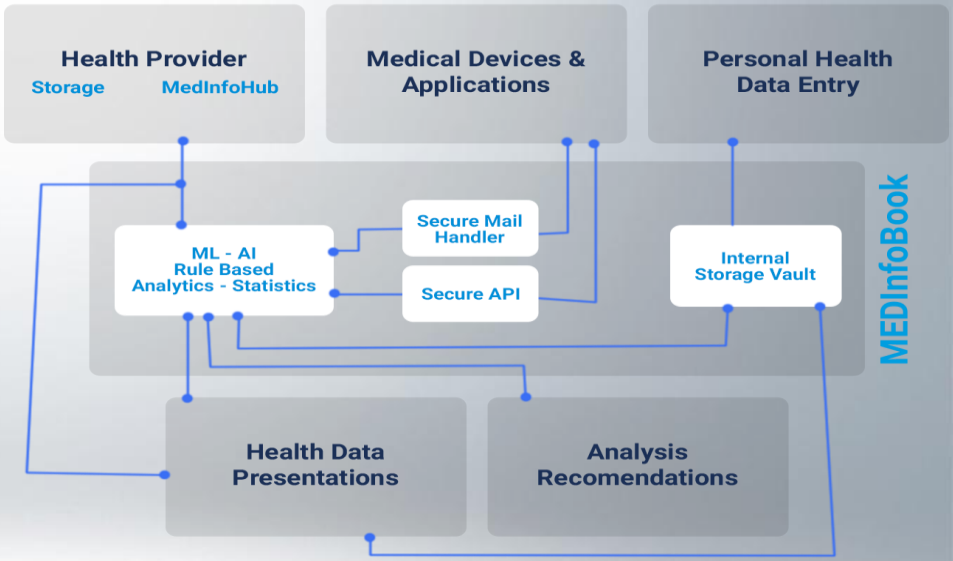
ΚΙΝΔΥΝΟΣ




4.5.2016
EN
Official Journal of the European Union
L 119/1
I
REGULATIONS
Insurer
Nurse
Doctor
Utilization Review
Patient
Surgeon
Dentist
Doctor
(Text with EEA relevance)
THE EUROPEAN PARLIAMENT AND
THE EUROPEAN UNION,

Computer Solutions
INTEGRATED INFORMATION SYSTEMS

MEDINFOBOOK
Medical Information Record

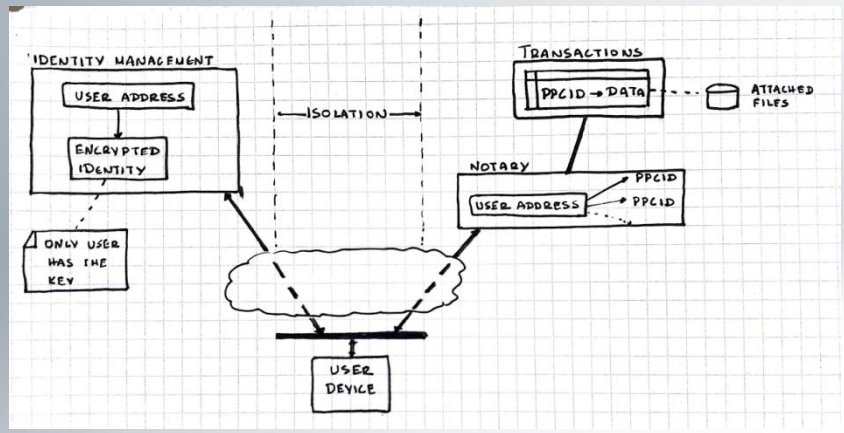


Article 25

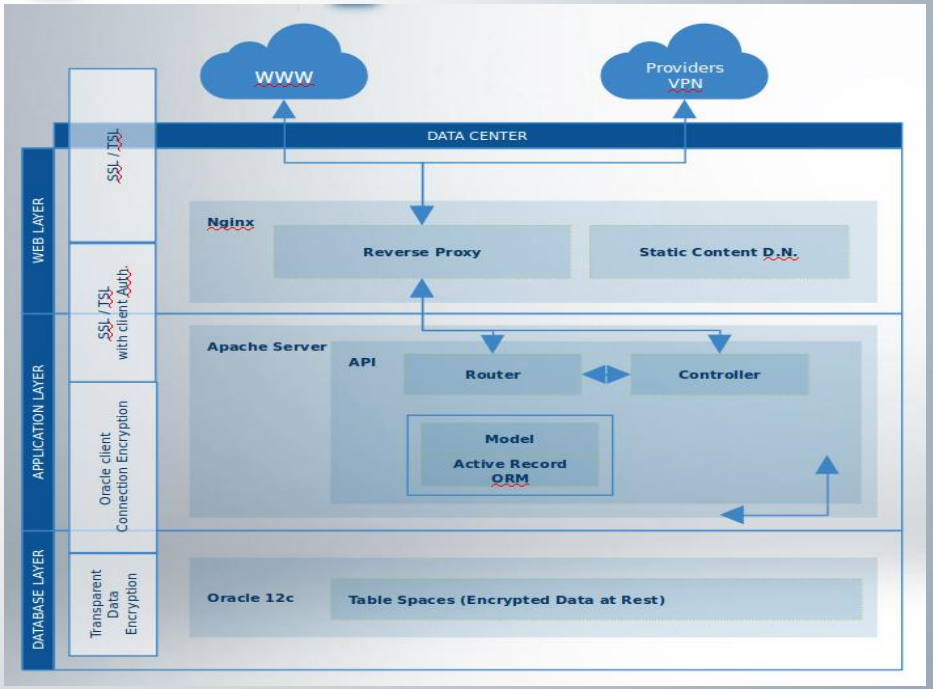
Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, 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, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.



MEDINFOBOOK
Medical Information Record



The final goal of the proposed architectural design can be described with approaches of different angles of attack on the issue of patient privacy:

- A system that even the maintainers and the database administrators have absolutely no way of knowing the identity of the person that own any piece of data in it (the system)
- A system that, even when fully compromised (the situation in which the potential perpetrator gains full control over the systems internals, code and database), the maximum information disclosed are clusters of transactional data for which he (the perpetrator) can only deduce that they belong to the same physical person, without having any means to extract info for this person's exact identity.

Article 20

Right to data portability

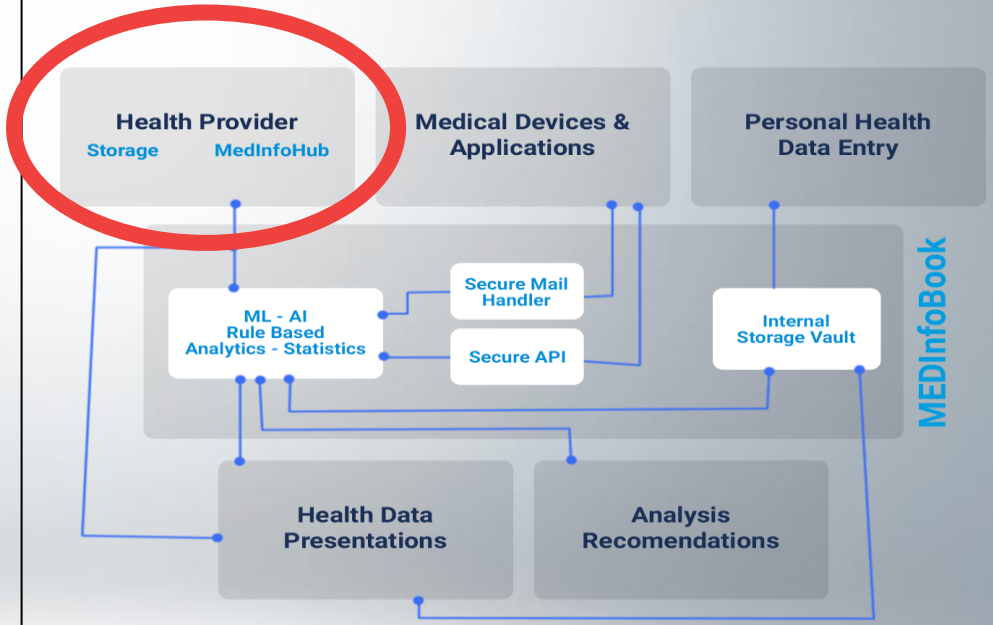
1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

MEDINFOBOOK
Medical Information Record



Article 7

Conditions for consent

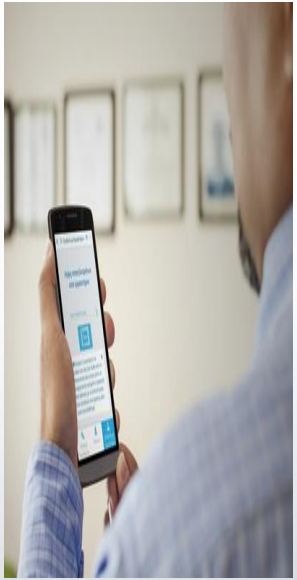
1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

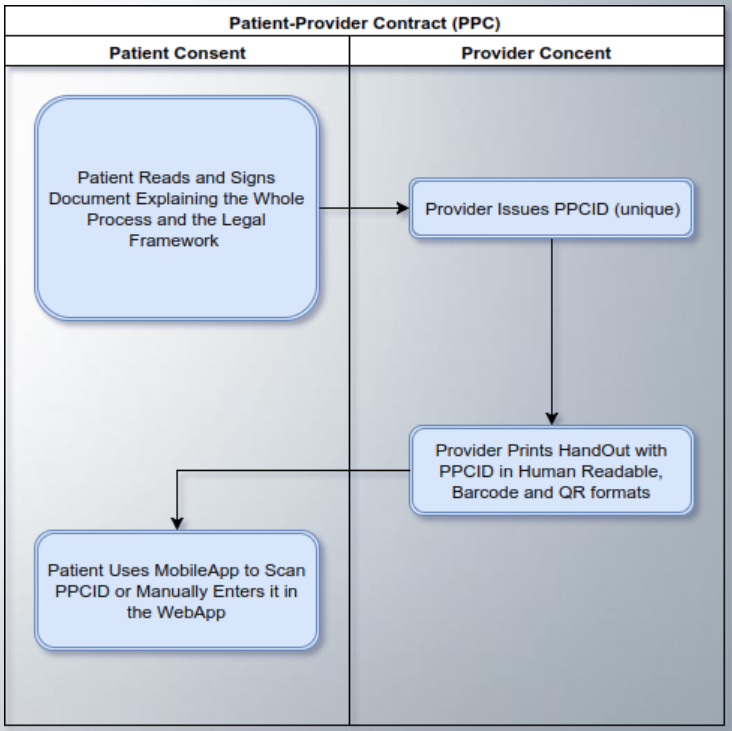
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

MEDINFOBOOK
Medical Information Record





We make sure that:

- Data from not-explicitly-consenting individuals will not participate in any transfer and will not be stored centrally.
- There is an unique identifier/token that cannot be tracked back to the individual's personal identifying data [Provider's security disclaimer] in the contaxt of the centralize PHR, that will always be used for data-in-transit (communication between provider's system and PHR) and data-at-rest (stored in the PHR's database).


SECURE HEALTH DATA
Computer
Solutions
INTEGRATED INFORMATION SYSTEMS
MEDI
V.01