ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Eurobank

Secure HealthData

ΑΣΦΑΛΕΙΑ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΥΓΕΙΑ

"Η εφαρμογή του GDPR στην πρωτοβάθμια φροντίδα υγείας, παρόν, προκλήσεις και προοπτικές"


# Αθανασιάδης Αντώνιος

Τεχνολόγος Ιατρικών Εργαστηρίων – Msc Διοίκησης Μονάδων Υγείας, Κ.Υ. Εχίνου

# Η εφαρμογή του GDPR στην πρωτοβάθμια φροντιδα υγείας. Παρόν, προκλήσεις και προοπτικές

Αθανασιάδης Αντώνιος
Τεχνολόγος Ιατρικών Εργαστηρίων
(Π.Ε.Δ.Υ) Κ.Υ. Εχίνου
Msc Διοίκησης Μονάδων Υγείας

# ΕΙΣΑΓΩΓΗ – ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Στον χώρο της περίθαλψης η πρώτη αναφορά για την προστασία των προσωπικών δεδομένων διατυπώθηκε στον όρκο του Ιπποκράτη.

Στον κώδικα ιατρικής δεοντολογίας, στο άρθρο 13 και στις παραγράφους 1&2 περικλείονται, πέραν των ιατρών, όλοι όσοι κατέχουν πληροφορίες σχετικές με την υγεία ενός ατόμου.

Με τον νόμο 2472/1997 γίνεται αναφορά για την τήρηση ηλεκτρονικού ιατρικού φακέλου.

Με τον 3235/2004 γίνεται εισαγωγή του όρου της ηλεκτρονικής κάρτας υγείας.

Με το άρθρο 51 του 4238/2014 καθιερώνεται η ηλεκτρονική κάρτα υγείας, η οποία αντικαθιστά το βιβλιάριο υγείας. Παράλληλα, ο νόμος 4213/2013 προέβλεπε τη συγκρότηση Εθνικού Συμβουλίου Διακυβέρνησης της Ηλεκτρονικής Υγείας (ΕΣΔΗΥ) και το Δίκτυο Ηλεκτρονικών Υπηρεσιών Υγείας (ΔΗΥΥ).

# ΑΠΟ ΤΗΝ ΟΔΗΓΙΑ 95/46/ΕΚ, ΣΤΟΝ ΚΑΝΟΝΙΣΜΟ 2016/679 (GPDR)

Οι ραγδαίες τεχνολογικές εξελίξεις, η ευρεία πρόσβαση στο διαδικτύου, οι υπηρεσίες υπολογιστικών νεφών (cloud) δημιούργησαν κενά στον προηγούμενο κανονισμό, καθιστώντας τον ξεπερασμένο και αναποτελεσματικό. (1) Στην εποχή των big data, ο Κανονισμός στοχεύει στην μεγίστη προστασία των δεδομένων προσωπικού χαρακτήρα από την όποια επεξεργασία στην οποία υποβάλλονται.

« *Τα φυσικά πρόσωπα θα πρέπει να έχουν τον έλεγχο των δικών τους δεδομένων προσωπικού χαρακτήρα. Θα πρέπει να ενισχυθούν η ασφάλεια δικαίου και η πρακτική ασφάλεια για τα φυσικά πρόσωπα, τους οικονομικούς παράγοντες και τις δημόσιες αρχές*» (2)

# ΣΤΟΧΟΙ GPDR

Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων που το αφορούν.

Η επεξεργασία τους θα πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο.

Η επίτευξη ενός ομοιογενούς χώρου ελευθερίας ασφάλειας και δικαιοσύνης, στον οποίο θα διακινούνται ελεύθερα τα προσωπικά δεδομένα, ανάμεσα στα κράτη μέλη.

# ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

*"Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου."*

«**Γενετικά δεδομένα**»**:** τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου,

«**Βιομετρικά δεδομένα**»**:** δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα,

«**Δεδομένα που αφορούν την υγεία**»**:** δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

# ΔΙΚΑΙΩΜΑΤΑ ΑΣΘΕΝΩΝ (ΥΠΟΚΕΙΜΕΝΩΝ)

- ΕΝΑΝΤΙΩΣΗΣ
- ΠΡΟΣΒΑΣΗΣ
- ΔΙΟΡΘΩΣΗΣ
- ΕΝΗΜΕΡΩΣΗΣ
- ΠΕΡΙΟΡΙΣΜΟΥ ΕΠΕΞΕΡΓΑΣΙΑΣ
- ΦΟΡΗΤΟΤΗΤΑΣ ΔΕΔΟΜΕΝΩΝ
- ΜΗ ΥΠΑΓΩΓΗΣ ΣΕ ΑΥΤΟΜΑΤΗ ΛΗΨΗ ΑΠΟΦΑΣΕΩΝ

**Κάθε δικαίωμα των ασθενών αποτελεί ένα υσμα για την βελτιστοποίηση των παρεχόμενων υπηρεσιών σε ένα κλίμα ασφάλειας, διαύγειας και υπευθυνότητας.**

# προϋποθέσεις νομιμότητας

Ο GDPR ορίζει **έξι προϋποθέσεις "νομιμότητας"** της επεξεργασίας και απαιτεί να ισχύει **τουλάχιστον μία** (Άρθρο 6).

- Το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία
- Η επεξεργασία είναι απαραίτητη για εκτέλεση σύμβασης (όπου το υποκείμενο είναι συμβαλλόμενος) ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου πριν τη σύναψη σύμβασης
- Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,
- Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος (του υποκειμένου ή άλλου φυσικού προσώπου),
- Η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας (που έχει ανατεθεί στον υπεύθυνο επεξεργασίας),
- Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος (..). Εξαιρούνται οι δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

# Η ΚΑΤΑΣΤΑΣΗ ΣΗΜΕΡΑ

Οι ιατρικοί φάκελοι (όπου υπάρχουν) τηρούνται και συντάσσονται με χειρόγραφο τρόπο, έχουν μεγάλο όγκο, δεν είναι σαφείς, δεν μπορούν εύκολα να εντοπιστούν, δεν μπορούν εύκολα να διαβαστούν.

Παρατηρείται το φαινόμενο ιατρικοί φάκελοι να έχουν χαθεί, ενώ πολλοί από εκείνους που υπάρχουν, είτε είναι φθαρμένοι είτε αλλοιωμένοι. (3)

Όπου υπάρχουν δεδομένα σε ψηφιακή μορφή, είναι καταχωρημένα τοπικά. Υπάρχει πληθώρα λογισμικών, τα οποία όμως δεν διασυνδέονται λόγω ετερογένειας. Ακόμα και εντός δομών υγείας τα δεδομένα δεν είναι προσβάσιμα από όλα τα τμήματα (4) (5)

# Επίπεδο ασφάλειας

Σε θέματα ασφάλειας η Αρχή Προστασίας Προσωπικών Δεδομένων, κατόπιν ελέγχων (Ν.2472/97), διαπίστωσε: [3] [6]

Μη ενεργοποίηση ηλεκτρονικών πρωτοκόλλων ασφαλείας σε επαρκή βαθμό. (Παλαιό λογισμικό το οποίο δεν υποστηρίζεται πλέον πχ windows xp)

Ελλιπές επίπεδο προστασίας χώρων φύλαξης

Ανυπαρξία ή ανεπάρκεια πολιτικών ασφαλείας, ελέγχου και οργάνωσης και δευτερευόντως ελλείψεις υλικοτεχνικού εξοπλισμού

Το 2015 μελέτη του Ευροβαρόμετρου κατέδειξε πως οι περισσότεροι πολίτες δεν έχουν τον έλεγχο σε ότι αφορά τα προσωπικά τους δεδομένα, ενώ σε ποσοστό 75% εμπιστεύονται τον τρόπο διαχείρισης από τις υπηρεσίες υγείας. [7]

# ΜΕΣΑ ΑΠΟΘΗΚΕΥΣΗΣ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΦΑΚΕΛΟΙ (DARK DATA),

ΨΗΦΙΑΚΑ ΜΕΣΑ (τοπικά ή σε δίκτυο)

- Παραβίαση χώρου φύλαξης

- Απώλεια, καταστροφή

- Προσπέλαση από μη εξουσιοδοτημένο προσωπικό

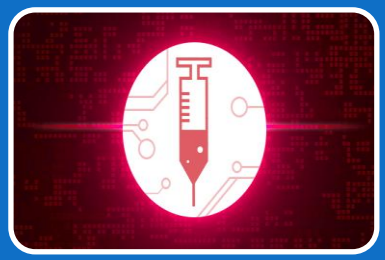

- Λανθασμένες καταχωρήσεις

# ΠΟΙΟΙ ΠΑΡΑΓΟΥΝ ΚΑΙ ΧΕΙΡΙΖΟΝΤΑΙ ΙΑΤΡΙΚΑ ΔΕΔΟΜΕΝΑ

- ΓΙΑΤΡΟΙ
- ΝΟΣΗΛΕΥΤΙΚΟ ΠΡΟΣΩΠΙΚΟ
- ΔΙΟΙΚΗΤΙΚΟ ΠΡΟΣΩΠΙΚΟ
- ΕΡΓΑΣΤΗΡΙΑΚΟ ΠΡΟΣΩΠΙΚΟ
- ΦΑΡΜΑΚΕΙΟ

# ΓΙΑΤΙ ΑΠΟΤΕΛΟΥΝ ΣΤΟΧΟ ΤΑ ΙΑΤΡΙΚΑ ΔΕΔΟΜΕΝΑ

**ΟΙΚΟΝΟΜΙΚΟ ΩΦΕΛΟΣ:** Η ¨αξία¨ ενός πλήρους ιατρικού φακέλου μπορεί να ανέλθει στα 1000 δολάρια. Τα στοιχεία του μπορεί να χρησιμοποιηθούν για παράνομη συνταγογράφηση. (8) (9)



**ΠΟΛΙΤΙΚΟ ΩΦΕΛΟΣ:** Οι ιστοσελίδες των οργανισμών υγείας λόγω της υψηλής επισκεψιμότητας αποτελούν στόχο κυβερνοεπιθέσεων προπαγανδιστικού περιεχομένου. (10) (11)

**ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ:** Οι δαπάνες για συστήματα ασφάλειας είναι μειωμένες, καθιστώντας τα εύκολους στόχους. (11)

# ΕΥΑΛΩΤΑ ΣΗΜΕΙΑ

## ΧΡΗΜΑΤΟΔΟΤΗΣΗ

Η χρηματοδότηση συστημάτων ασφάλειας βρίσκεται συνήθως σε ¨δεύτερη¨ μοίρα.

## ΛΟΓΙΣΜΙΚΟ

Αρκετές μονάδες υγείας μπορεί να χρησιμοποιούν παλιές εκδόσεις λογισμικού (πχ windows xp ή και παλαιότερες εκδόσεις), οι οποίες δεν ενημερώνονται, ακόμα και στο NHS. (12) Επίσης αρκετά λογισμικά δεν έχουν ενεργοποιημένο το κατάλληλο επίπεδο ασφάλειας.

## ΧΡΗΣΤΕΣ

Η πρόσβαση σε " ύποπτες" ιστοσελίδες, το ηλεκτρονικό ψάρεμα (Phising), το άνοιγμα ενός ύποπτου mail, μπορεί να οδηγήσουν στην απώλεια δεδομένων προσφέροντας πύλη εισόδου σε χάκερ.

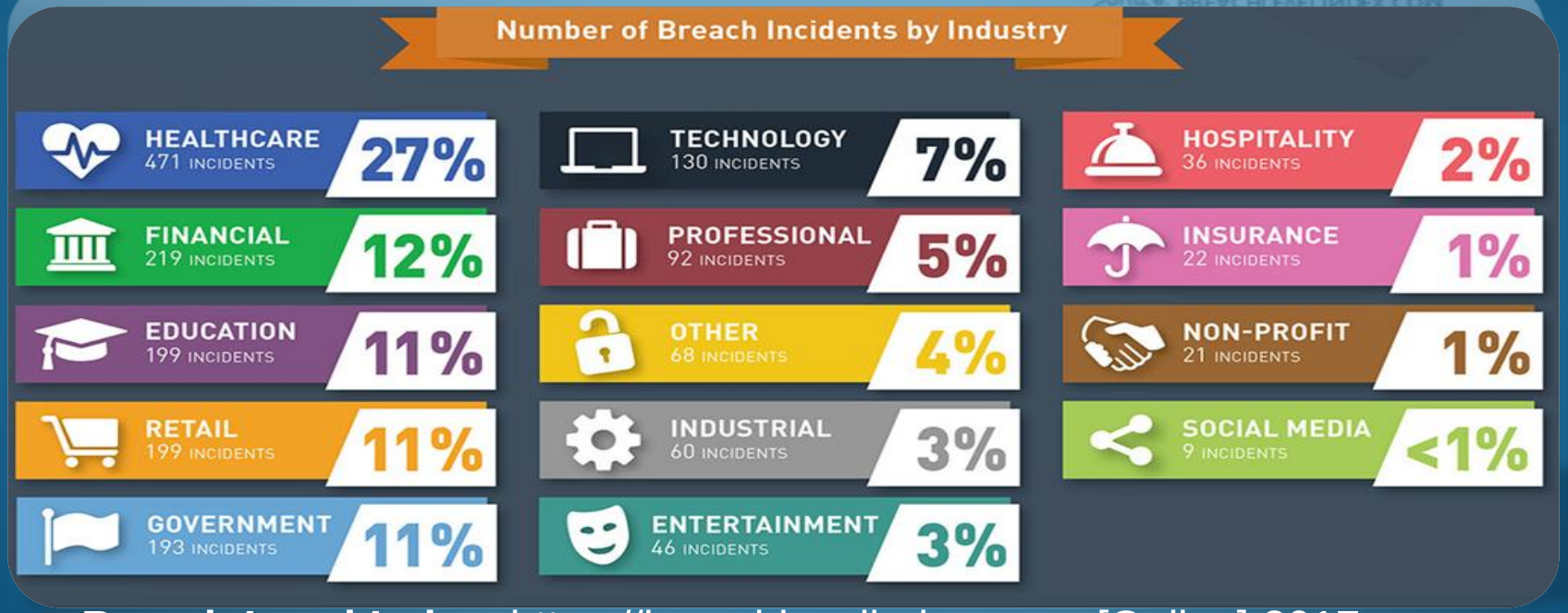
## ΧΡΗΣΗ ΣΥΣΚΕΥΩΝ

Η χρήση τόσο κινητών συσκευών (κινητά, τάμπλετ), αλλά και αρκετές ιατρικές συσκευές οι οποίες συνδέονται με πληροφοριακά συστήματα, αποτελούν πύλες εισόδου. (11)

# NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

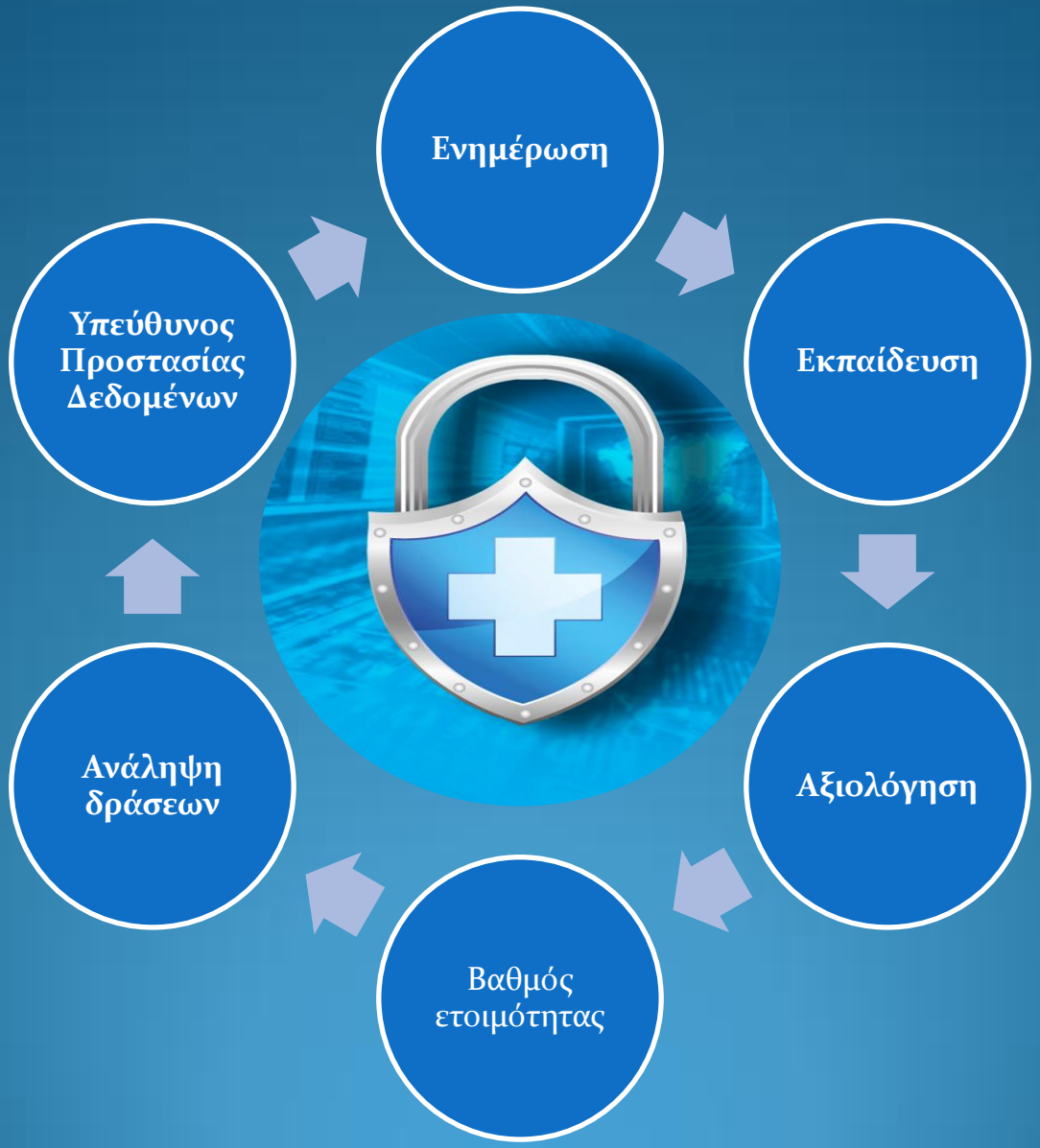
| INDUSTRY | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|
| Healthcare | 346 | 449 | 451 | 531 | 471 |
| Financial Services | 166 | 213 | 276 | 241 | 219 |
| Retail | 97 | 197 | 240 | 247 | 199 |
| Education | 36 | 174 | 166 | 166 | 199 |
| Government | 196 | 293 | 299 | 289 | 193 |
| Technology | 112 | 140 | 124 | 203 | 130 |
| Professional Services | - | 1 | 1 | 1 | 92 |
| Other Industries | 263 | 275 | 316 | 160 | 68 |
| Industrial | - | - | - | 32 | 60 |
| Entertainment | - | - | 5 | 31 | 46 |
| Hospitality | 1 | 1 | 2 | 35 | 36 |
| Insurance | - | - | 2 | 15 | 22 |
| Non-Profit | - | - | - | 28 | 21 |
| Social Media | - | 1 | 2 | 2 | 9 |
| TOTALS | 1,217 | 1,743 | 1,883 | 1,981 | 1,765 |

Source: BREACHLEVELINDEX.COM




**Breach Level Index.** https://breachlevelindex.com. [Online] 2017.

# Βήματα προς τον GPDR



# ΠΡΟΟΠΤΙΚΕΣ

Ήδη έχει ξεκινήσει ο θεσμός του οικογενειακού γιατρού, αρμοδιότητα του οποίου είναι να τηρεί τον ατομικό ιατρικό φάκελο των ασθενών. Η μετάβαση στην ψηφιακή πλέον εποχή, θα διευκολύνει το έργο των επαγγελματιών υγείας:

-στην παροχή υψηλού βαθμού υπηρεσιών υγείας

-μείωση και έλεγχο δαπανών

-καλύτερη παρακολούθηση χρόνιων νοσημάτων

-αίσθημα ασφάλειας και εμπιστοσύνης

Η εφαρμογή του νέου κανονισμού προστασίας προσωπικών δεδομένων δίνει την ευκαιρία να οικοδομηθεί ορθά ο ιατρικός φάκελος.

# Προκλήσεις

Η μεγαλύτερη πρόκληση είναι η μετάβαση από την αδράνεια στην πράξη, την καινοτομία και την εξέλιξη.

Οι βάσεις, όπως η ύπαρξη ενός ασφαλούς δικτύου, κρυπτογράφησης και ψηφιακών υπογραφών - κλειδιών υπάρχουν. (ΣΥΖΕΥΞΙΣ)

Η διατήρηση και προφύλαξη των δεδομένων μπορεί να επιτευχθεί με ενίσχυση ή αναβάθμιση των υποδομών. Εφαρμογή προτύπου (iso 27001)

Η πλήρης ανάπτυξη, εφαρμογή και εξέλιξη του ιατρικού φακέλου, βάση των οδηγιών του κανονισμού, μπορεί να επιλύσει τα υπάρχοντα προβλήματα ετερογένειας. Σε συνδυασμό με τεχνολογίες κρυπτογράφησης, το ιατρικό ιστορικό μπορεί να έχει διαβαθμισμένη και ελεγχόμενη πρόσβαση , άμεσα και αξιόπιστα .

# Σας ευχαριστώ!

# Βιβλιογραφία


1. *Η επίδραση του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) στην επεξεργασία ιατρικών δεδομένων.* **Γρηγόρης Τσόλιας.** 2018. ΙΣΑ «Ο νέος Κανονισμός για την προστασία προσωπικών δεδομένων στις ιδιωτικές δομές υγείας».

2. *ΚΑΝΟΝΙΣΜΟΣ 2016/679.* Επίσημη Εφημερίδα Ευρωπαϊκής Ένωσης,, σ. L119/2 παρ.7.

3. **Ψαρούλης Δ.,Βούλτσος Π.,** *Ιατρικό Δίκαιο, Στοιχεία Βιοηθικής.* Αθήνα : University Studio Press., 2010.

4. **Γαλάνης Π.,.** *Μεθοδολογία Ανάλυσης Δεδομένων στις Επιστήμες Υγείας.* Αθήνα : Πασχαλίδης, 2015. σσ. 76-88.

5. **Τσιριντάνη Μ.** *Βάσεις Δεδομένων και Πολυμέσα στην Υγεία.* Αθήνα : Πασχαλίδης, 2012. σσ. 49-58.

6. **Μητροσύλη Μ.** *Δίκαιο της Υγείας.* Αθήνα : Παπαζήση, 2009. σσ. 44-52.

7. **EUROBAROMETER.** *Special Eurobarometer 431 " DATA PROTECTION".* [Online] 2015. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf. p:63-65.

8. *NHS cyber attack: why stolen medical information is so much more valuable than financial data.* **Sulleyman A.** 2017, The Independent.

9. *Justice Department Files Record $900 Million Healthcare Fraud Case,.* **Berlinger J.** 2016, CNN.

10. *Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images.* **Sengupta K.** 2017, Independed.

11. **Snell E.** Hacking still leading cause of 2015. *Health IT seq.* 2015.

12. **Lynne Coventry, Dawn Branley.** Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas.* 2018, 113.

13. **Milliman R.,.** Nine in 10 NHS trusts still use windows XP. *IT Pro.* 2016.

14. **Breach Level Index.** https://breachlevelindex.com. [Online] 2017. https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf. pg:11.