ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Eurobank

Secure HealthData

ΑΣΦΑΛΕΙΑ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΥΓΕΙΑ

"Η χαρτογράφηση των προσωπικών δεδομένων στο Νοσοκομείο"

Κεσανλή Φωτεινή

Υπάλληλος Στατιστικής Msc, Τμήμα Πληροφορικής – Γενικό Νοσοκομείο Ξάνθης

Χαρτογράφηση προσωπικών δεδομένων στο Νοσοκομείο

Φωτεινή Κεσανλή,Στατιστικός MSc,
Υπάλληλος Γ. Ν. Ξάνθης

Secure HealthData

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Ιστορία

- Τον Ιανουάριο του 1981 υπογράφηκε στο Στρασβούργο η Ευρωπαϊκή Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα
- Με τον Ν. 2068/1992 γίνεται η Κύρωση της Ευρωπαϊκής Σύμβασης και ισχύει για το Ελληνικό Κράτος
- Το πρώτο νομοθετικό κείμενο στην χώρα μας Ν.2472/1997 – Ενσωμάτωση της Οδηγίας 95/46/ΕΚ: Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα - Σύσταση ΑΠΔΠΧ

Ιστορία

Έκτοτε έχουν γίνει διάφορες τροποποιήσεις για την ενσωμάτωση επόμενων οδηγιών της ΕΕ

- Ελληνική Νομοθεσία
  - Νόμος 3471/2006
  - Νόμος 3783/2009
  - Νόμος 3917/2011
  - Νόμος 4070/2012
  - 1998-2011 Κανονιστικές πράξεις της ΑΠΔΠΧ

- Ευρωπαϊκή Νομοθεσία
  - Οδηγία 2002/58/ΕΚ
  - Οδηγία 2006/24/ΕΚ
  - Οδηγία 2009/136/ΕΚ

→ Κανονισμός (ΕΕ) 2016/679 (GDPR)

Οδηγία (ΕΕ) 2016/680, Οδηγία (ΕΕ) 2016/681

Προσδιορισμός των βασικών στοιχείων

Στοιχεία προσωπικών δεδομένων	Μορφές δεδομένων	Μέθοδοι μεταφοράς δεδομένων	Τοποθεσία δεδομένων
• Όνομα, διεύθυνση, e-mail • Δεδομένα υγείας, ποινικό μητρώο • Βιομετρικά δεδομένα, δεδομένα θέσης	• Σε έντυπη μορφή • Σε απεικονιστική μορφή • Ηχητικά • Σε ψηφιακή μορφή • Οργανωμένα σε Βάσεις Δεδομένων	• Εσωτερική (εντός νοσηλ. Μονάδας) • Εξωτερική (εκτός νοσηλ. Μονάδας) • Ταχυδρομείο, τηλέφωνο, e-mail	• Γραφεία • Τοπικούς σταθμούς εργασίας (Η/Υ) • Φορητές μονάδες αποθήκευσης δεδομένων (cd, usb) • Servers • Cloud

Οι βασικές προκλήσεις της χαρτογράφησης προσωπικών δεδομένων στο Νοσοκομείο

- Η πρώτη πρόκληση είναι να αποφασιστεί ποιες πληροφορίες πρέπει να καταγραφούν και σε ποια μορφή.
- Η δεύτερη πρόκληση είναι να προσδιοριστεί η κατάλληλη τεχνολογία, η πολιτική και οι διαδικασίες για τη χρήση και την προστασία των πληροφοριών, ενώ παράλληλα να καθορίζεται ποιος ελέγχει την πρόσβαση σε αυτές.
- Η τελευταία πρόκληση είναι να καθοριστεί ποιες είναι οι νομικές και κανονιστικές υποχρεώσεις του οργανισμού.

Παράδειγμα ροής πληροφοριών - Ασθενής κατά την προσέλευση στα ΤΕΠ

Προσωπικά δεδομένα:

- Ονοματεπώνυμο
- Διεύθυνση
- Τηλέφωνο
- ΑΜΚΑ
- Ασφαλιστικός φορέας
- Τρόπος προσέλευσης

Προσωπικά Δεδομένα

Πρόσβαση:

- Διοικητικό Προσωπικό γραμματείας
- Πιθανοί Λοιποί Παρευρισκόμενοι

Secure HealthData

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Ασθενής κατά την Ιατρική εξέταση στα ΤΕΠ

Προσωπικά δεδομένα:

- Προσωπικά Δεδομένα
- Κλινικά ευρήματα

} Ευαίσθητα Προσωπικά Δεδομένα

Πρόσβαση:

- Ιατρός
- Νοσηλευτικό προσωπικό
- Πιθανοί Λοιποί Παρευρισκόμενοι

Εξετάσεις Ασθενή στα Εργαστήρια

Προσωπικά Δεδομένα

- Ευαίσθητα Προσωπικά Δεδομένα
- Αιτούμενη εξέταση
- Γενετικές πληροφορίες (π.χ. αίμα)

Πρόσβαση:

- Ιατρικό Προσωπικό
- Νοσηλευτικό Προσωπικό
- Παραϊατρικό Προσωπικό
- Πιθανοί Λοιποί Παρευρισκόμενοι

Secure HealthData

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Ασθενής σε Νοσηλεία

Προσωπικά δεδομένα:

- Ευαίσθητα Προσωπικά Δεδομένα
- Γνωμάτευση εισόδου
- Ιστορικό
- Αποτελέσματα εξετάσεων

Πρόσβαση:

- Ιατρικό Προσωπικό Κλινικής
- Νοσηλευτικό Προσωπικό Κλινικής
- Γραμματεία Κλινικής
- Βοηθητικό Προσωπικό Νοσοκομείου
- Επισκεπτήριο
- Προσωπικό Εστίασης

Ασθενής στο Εξιτήριο

Προσωπικά δεδομένα:

- Ευαίσθητα Προσωπικά Δεδομένα
- Διάγνωση Εξόδου
- Ιατρικές Πράξεις
- Οδηγίες Εξόδου

Πρόσβαση:

- Ιατρικό Προσωπικό Κλινικής
- Νοσηλευτικό Προσωπικό Κλινικής
- Γραμματεία Κλινικής
- Διοικητικό Προσωπικό Τμήματος Κίνησης Ασθενών

Παράδειγμα - Εργαζόμενος

Προσωπικά δεδομένα:

- Προσωπικά Στοιχεία
- Περιουσιακά Στοιχεία
- Κρίσεις και Υπηρεσιακές Μεταβολές
- Αναρρωτικές και Άλλες Άδειες
- Ποινές και Αναφορές

Πρόσβαση:

- Προσωπικό Τμήματος Διαχείρισης Ανθρώπινου Δυναμικού

Κίνδυνοι προσωπικών δεδομένων

Διαρροή	Αλλοίωση	Απώλεια
• Από ακούσια κοινοποίηση • Λόγω διαμόρφωσης χώρων που δεν προστατεύουν την ατομικότητα • Λόγω διαδικασιών	• Από ανθρώπινο λάθος • Λόγω έλλειψης γραμματείας κατά τις νυχτερινές ώρες • Λόγω διαδικασιών ταυτοποίησης	• Από ανθρώπινο λάθος • Λόγω μη χρήσης αντιγράφων • Λόγω διαδικασιών

Μείωση των κινδύνων

Ανθρώπινος παράγοντας

- Κατανόηση της σοβαρότητας των προσωπικών δεδομένων
- Σεβασμός στην ατομικότητα
- Κατανόηση των κινδύνων από αμελή χρήση διαδικτύου
- Κατανόηση της πρόσβασης στο πληροφοριακό σύστημα

Υποδομές

- Χώροι που προστατεύουν την ατομικότητα
- Διαχωριστικά που προστατεύουν την ιδιωτική επικοινωνία
- Σύγχρονα συστήματα προστασίας πληροφοριακών συστημάτων

Διαδικασίες

- Προστασία των πληροφοριών που διακινούνται
- Εκσυγχρονισμός μεθόδων πρόσβασης στα δεδομένα
- Σύνταξη μεθοδολογίας διαδικασιών και ανάπτυξη μηχανισμών παρακολούθησης
- Διαδικασία εκτίμησης κινδύνου και τρόποι αντίδρασης

Δικαιώματα πολιτών

- Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα (αρ. 12 & 15)
- Δικαίωμα διόρθωσης (αρ. 16)
- Δικαίωμα περιορισμού της επεξεργασίας (αρ. 18)
- Δικαίωμα εναντίωσης στην επεξεργασία (αρ. 21)
- Δικαίωμα στη λήθη (αρ. 17)
- Δικαίωμα στη φορητότητα των δεδομένων (αρ. 20)

Secure HealthData

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Δικαίωμα ενημέρωσης και πρόσβασης άρθρα 12 & 15

Ο γιατρός/Νοσοκομείο υποχρεούται να τηρεί ιατρικό αρχείο (Ν. 3418/2005 αρ. 14)

↓

Τήρηση αρχείου (βλ. διατάξεις Ν. 2472/1997)

↓

Ισχύς αρχείου

10 έτη για τα ιδιωτικά ιατρεία και ιδιωτικές ΜΠΦΥ	20 έτη σε κάθε άλλη περίπτωση

↓

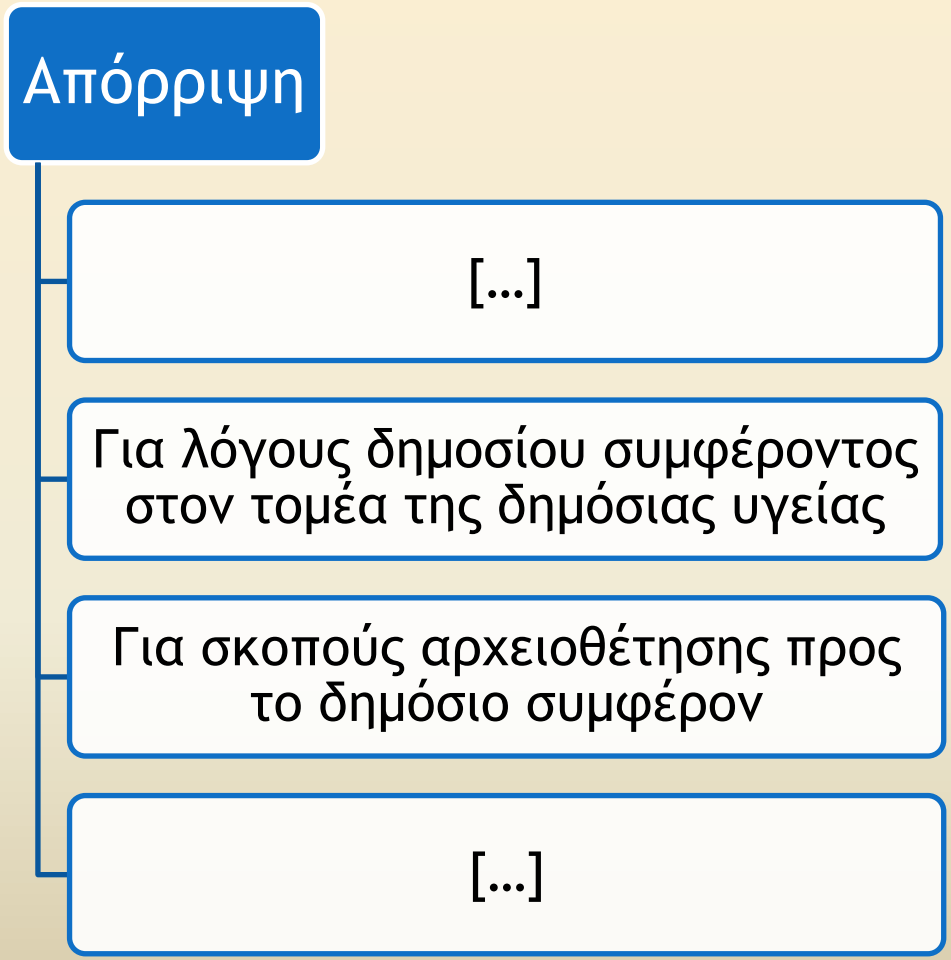
Δικαίωμα πρόσβασης

Ασθενής	Νόμιμοι εκπρόσωποι	Κληρονόμοι	Ελληνική πολιτεία (Ν.3418/2005 αρ.14 παρ.9)

SecureHealthData

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Δικαίωμα στη λήθη άρθρο 17 παρ. 3



Διατήρηση αρχείων

Νομοθεσία

- ΠΔ 162-ΦΕΚ 42/Α/06.03.1979
- ΠΔ 768-ΦΕΚ 186/Α/18.08.1980
- ΠΔ 11-ΦΕΚ 7/Α/09.01.1981
- ΠΔ 87-ΦΕΚ 27/Α/03.02.1981
- ΠΔ 1258-ΦΕΚ 309/Α/16.10.1981
- ΠΔ 480-ΦΕΚ 173/14.10.1985

Εφαρμογή

- Πρακτικά Υγειονομικών Επιτροπών: 5
- Μητρώα ασθενών: 50
- Μητρώα ασθενών χρονίως πασχόντων: στο Διηνεκές
- Φάκελοι ασθενών: 20
- Έτερα στοιχεία αφορούντα τη διακίνηση των ασθενών (ασφαλιστικός οργανισμός, κ.λπ.): 3
- Βιβλία λογοδοσίας κλινικών: 5
- Βιβλία Εξωτερικών Ιατρείων: 5
- Βιβλία χειρουργικών επεμβάσεων: 15

Secure HealthData

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Διατήρηση αρχείων

Νομοθεσία

- ΠΔ 162-ΦΕΚ 42/Α/06.03.1979
- ΠΔ 768-ΦΕΚ 186/Α/18.08.1980
- ΠΔ 11-ΦΕΚ 7/Α/09.01.1981
- ΠΔ 87-ΦΕΚ 27/Α/03.02.1981
- ΠΔ 1258-ΦΕΚ 309/Α/16.10.1981
- ΠΔ 480-ΦΕΚ 173/14.10.1985

Εφαρμογή

- Μισθολογικά Μητρώα υπαλλήλων: 20
- Ατομικοί υπηρεσιακοί φάκελοι μη συνταξιοδοτηθέντων υπαλλήλων: 5 από την αποχώρησή τους
- Ατομικοί φάκελοι συνταξιοδοτηθέντων υπαλλήλων: όσο καταβάλλεται η σύνταξη
- Βιβλία ασθενειών και αδειών υπαλλήλων: 5
- Αιτήσεις και αναφορές υπαλλήλων: 2

Δικαιώματα πολιτών στην Υγεία

Ο ασθενής ή ο νόμιμος εκπρόσωπος

- Ενημέρωση και πρόσβαση στα δεδομένα
- Διόρθωση
- Περιορισμό επεξεργασίας λόγω κακόβουλης χρήσης
- Εναντίωση στην επεξεργασία λόγω εμπορικής προώθησης δεδομένων
- Φορητότητα

Από κανέναν

- Δικαίωμα στη λήθη (ισχύουσα νομοθεσία)

Εν αναμονή επίσημων οδηγιών

- Υπάρχει ισχύουσα νομοθεσία
- Υπάρχουν διαδικασίες
- Ο Ευρωπαϊκός Κανονισμός 2016/679 (GDPR) χρειάζεται εξειδίκευση
- Η υπερβολές δε λειτουργούν προς όφελος κανενός
- Αντίθετα η προσεκτικότερη αντιμετώπιση των εμπλεκομένων θα διευκολύνει την προσαρμογή

Secure HealthData

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Ευχαριστώ για την προσοχή σας!

Secure HealthData

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ