«Οι προϋποθέσεις εφαρμογής του νέου ΚΠΠΔ (GDPR) στην Ιατρική πράξη: Υποχρεώσεις κεντρικής Διοίκησης, ΗΔΙΚΑ, ΕΟΠΥΥ και επαγγελματιών Υγείας»

Χριστίνα Παπανικολάου
Βιοπαθολόγος
Πρόεδρος Τομέα Ηλεκτρονικής Υγείας και Διασυνοριακής Περίθαλψης ΙΕΕ – ΠΙΣ

Αθήνα, 28 - 04 - 2018

Ι. ΤΟ ΝΕΟ ΤΕΧΝΟΛΟΓΙΚΟ – ΨΗΦΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ ΣΤΗΝ ΥΓΕΙΑ

1. **Ο ψηφιακός μετασχηματισμός των Συστημάτων Υγείας και Κοινωνικής Προστασίας**

- **Πληροφοριακά Συστήματα** Μονάδων Υγείας
- **Ηλεκτρονικός Φάκελος** Ασθενούς ή Ηλεκτρονικός Φάκελος Υγείας (patient summary)
- **Ηλεκτρονική**, Εθνική ή Διασυνοριακή **Συνταγογράφηση**
- Ενσωμάτωση **συστημάτων υποβοήθησης λήψης ιατρικών αποφάσεων** (πρωτόκολλα, κατευθυντήριες οδηγίες)

…(Ψηφιακός Μετασχηματισμός Σ.Υ.)

- **Τηλεσυμβουλευτική** (on line συνεδρία ασθενούς / επαγγελματιών υγείας) ή μέσω τεχνολογίας **αισθητήρων** μετάδοσης Βιολογικών δεικτών και άλλων κλινικών δεδομένων
- **Τηλειατρική** (διαγνωστικοί, θεραπευτικοί, εκπαιδευτικοί σκοποί…)
- **“Mobile health” (m-health)** πολυάριθμες εφαρμογές μέσω κινητού τηλεφώνου
- **Precision medicine** (ρομποτική)

2. **Νέα μοντέλα κλινικής διαχείρισης ασθενών και ασθενειών, πρόληψης, πρόγνωσης, κ.λπ.**

- **Integrated care** (ολοκληρωμένη, συνεκτική φροντίδα)
- **Personalized medicine**
- **Evidence based medicine**

3. **Ραγδαία ανάπτυξη και χρήση εργαλείων και εφαρμογών ICT στην Υγεία**

- Big data analytics (ανάλυση μεγάλων, ενοποιημένων βάσεων δεδομένων)
- Νεφοϋπολογιστική (cloud)
- Τεχνολογία blockchain
- Τεχνητή νοημοσύνη

4. ICT: προώθηση ριζικών μεταρρυθμίσεων και αναδιαρθρώσεων των Σ.Υ.

- **Ενίσχυση δικτύωσης** μεταξύ διαφορετικών επιπέδων και τομέων Υγειονομικών Υπηρεσιών
- **Ενίσχυση σύγκλισης** μεταξύ Υπηρεσιών Υγείας και Υπηρεσιών Κοινωνικής προστασίας (Κοινωνική ασφάλιση, Πρόνοια)
- **Αξιοποίηση big data** για επιδημιολογικούς, ερευνητικούς, διαγνωστικούς και άλλους σκοπούς (ERN).
- **Διασφάλιση ποιότητας,** ασφάλειας, συνέχειας, διαθεσιμότητας Υπηρεσιών Υγείας προς τους πολίτες

- **Υποστήριξη βιωσιμότητας και αποδοτικότητας** των Συστημάτων Υγείας
- **Διευκόλυνση** διασυνοριακής περίθαλψης στην Ε.Ε. (οδηγία 24/11/Ε.Κ., Προστασίας δικαιωμάτων ασθενών στη διασυνοριακή περίθαλψη)

5. Μετάβαση σε «ασθενοκεντρικό» μοντέλο

- **Ενίσχυση της θέσης του ασθενούς** / χρήση Υπηρεσιών Υγείας μέσα στο Σύστημα
- Πληροφορημένες επιλογές, πρόσβαση στα ιατρικά δεδομένα, παρέμβαση στον Ατομικό Ηλεκτρονικό Φάκελο Υγείας, συγκατάθεση κτλ…

II. ΤΑ ΘΕΣΜΙΚΑ, ΤΕΧΝΙΚΑ ΚΑΙ ΔΙΑΔΙΚΑΣΤΙΚΑ ΠΡΟΒΛΗΜΑΤΑ ΕΦΑΡΜΟΓΗΣ ΤΟΥ GDPR

Υγειονομικός τομέας

Το μεγαλύτερο «εργαστήριο» παραγωγής, συλλογής, διακίνησης

ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΥΓΕΙΑΣ

- **Ορισμός** δεδομένων Υγείας (Αρ.4 ΓΚ)και Γενετικών δεδομένων
- «Ειδικές κατηγορίες» ή «ευαίσθητα» δεδομένα (Αρ.9 ΓΚ)

1. Γενικά προβλήματα προσαρμογής δημοσίων Αρχών, οργανισμών, επαγγελματιών Υγείας…

- Ελλειμματική ψηφιακή γνώση και εκπαίδευση – ενημέρωση (digital literacy)
- **Ελλείψεις** στην υιοθέτηση **ενιαίας εθνικής στρατηγικής Ηλεκτρονικής διακυβέρνησης στην Υγεία**
- **Ελλείψεις** σε στρατηγική **διαλειτουργικότητας** (χαρακτηριστικότερο παράδειγμα: ΗΦΥ)
- **Αδυναμίες εκσυγχρονιστικών μεταρρυθμίσεων** και ενσωμάτωσης καινοτομίας στο Υγειονομικό Σύστημα.
- Θεσμικά κενά και ασάφειες.

2. Τι αλλάζει ο GDPR

- Οδηγία 95/46 – Ν2472
- Κώδικας Ιατρικής Δεοντολογίας (Ν. 3418/2005)

i. **Διακριτοί ρόλοι και υποχρεώσεις υπεύθυνων και εκτελούντων την επεξεργασία ΔΠΧ**

ii. **Ενισχυμένα δικαιώματα ασθενών / χρηστών Υπηρεσιών Υγείας** (πρόσβαση, διόρθωση, συγκατάθεση, λήθη, φορητότητα, κ.λπ.)

iii. **Αποδείξεις συμμόρφωσης** στις απαιτήσεις των ΓΚΠΔ από υπεύθυνους και εκτελούντες, τεχνικά και οργανωτικά μέτρα για τη διασφάλιση «σύννομης και δίκαιης» επεξεργασίας

3. Μεγάλης Κλίμακας (Επεξεργασία «ευαίσθητων» ή «ειδικής κατηγορίας» δεδομένων

…Σύμφωνα με το ΓΚ: «Εκτελείται με νόμιμη υποχρέωση ή όσον αφορά εκπλήρωση δημοσίου ενδιαφέροντος ή άσκηση δημόσιας εξουσίας…» (αιτ. σκ. 10,45, Αρ. 9 ΓΚ)

«Δημόσιο συμφέρον»: Δημόσια Υγεία, κοινωνική προστασία, διαχείριση Υπηρεσιών Υγείας.

Δεν αποκλείεται Εθνική (τομεακή) Νομοθεσία με προηγούμενη διαβούλευση με την ΑΠΠΔ

- Μέτρα προσαρμογής στις Αρχές επεξεργασίας
- Καθορισμός ρόλων υπευθύνων και εκτελούντων

- Καθορισμός αποδεκτών κοινοποίησης ΔΠΧ
- Περιορισμός σκοπού
- Περίοδος αποθήκευσης
- Διαχείριση ΔΠΧ : - ταυτοποιήσιμων
  – ψευδονυμοποιημένων
  – ανωνυμοποιημένων
- Τεχνικά και οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων των ασθενών
- Μελέτες αντικτύπου (risk assessament)
- Πρότυπα, κωδικοποιήσεις, πιστοποίηση (certification), φορείς διαπίστευσης
- Διαδικασία και είδη συγκατάθεσης
- Περιορισμός και παρεκκλίσεις σε ειδικές περιπτώσεις

4. Προτάσεις ενδεχόμενων θεσμικών μέτρων

Α. Εξουσιοδότηση έκδοσης Υπουργικής Απόφασης (ΚΥΑ) στο νέο νομοθέτημα προσαρμογής της Ελληνικής νομοθεσίας (κατάργηση Ν. 2472)

ή

Β. Ενσωμάτωση κεφαλαίου ειδικών ρυθμίσεων για την υγεία

Γ. Επικαιροποίηση ή/και συμπλήρωση του Κώδικα Ιατρικής Δεοντολογίας (Ν. 3418/2005)

(διαβούλευση με την ΑΠΠΔ)

Δ. Πρόβλεψη ειδικών συμβάσεων μεταξύ υπευθύνων επεξεργασίας, δηλαδή ΗΔΙΚΑ, ΕΟΠΥΥ, Υπουργείο Υγείας και **εκτελούντων** (Μονάδες και επαγγελματίες υγείας) (αιτ. σκ. 81)

Ειδικές προβλέψεις για ενδεχόμενες παραβιάσεις της ασφάλειας των δικτύων και κλοπής ιατρικών δεδομένων (cyber security)

Ε. Χρηματοδότη προσαρμογής από εθνικούς ή/και κοινοτικούς πόρους

III. ΕΙΔΙΚΟΤΕΡΕΣ ΡΥΘΜΙΣΕΙΣ ΓΙΑ ΤΗΝ ΠΡΟΣΑΡΜΟΓΗ ΤΟΥ GDPR ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΝΟΜΟΘΕΤΗΘΟΥΝ

1. **Παρεκκλίσεις από την απαγόρευση επεξεργασίας δεδομένων Υγείας και Γενετικών δεδομένων** (αιτ. σκ. 52-53-54 και Αρ. 9 ΓΚ)

- Υγειονομική ασφάλεια
- Δημόσια Υγεία (1338/08 ΕΚ)
- Διαχείριση ποιότητας, αποδοτικότητας, κόστους, κ.λπ., Υπηρεσιών Υγείας και Κοινωνικής Ασφάλισης
- Επιστημονικοί και στατιστικοί σκοποί

«Επεξεργασία με ευθύνη επαγγελματία που υπόκειται στην υποχρεωτική τήρηση επαγγελματικού απορρήτου…»

2. Προσδιορισμός «νομιμότητας επεξεργασίας» για τα δεδομένα Υγείας και τα Γενετικά δεδομένα

- Προϋποθέσεις συγκατάθεσης
- «Συγκατάθεση παιδιού» (Άρθρα 6, 7 & 8 του ΓΚ)

(…..«τα ΚΜ μπορεί να θεσπίζουν πιο ειδικές διατάξεις…» (Άρ. 6, παρ. 2)

3. Δικαιώματα ασθενών/χρηστών

- **Ενημέρωση και πρόσβαση** (Άρ. 13-15)
  (συλλογή δεδομένων)
- **Διόρθωση και διαγραφή** (ή «λήθη»)
- Επιλεκτική θωράκιση δεδομένων, φαινοτυπικά και γονοτυπικά δεδομένα
- **Δικαίωμα εναντίωσης στην αυτοματοποιημένη λήψη αποφάσεων**

✓ Εφαρμογές: **Πρωτόκολλα** διαγνωστικά και θεραπευτικά

✓ Άλλες ψηφιακές εφαρμογές (m-health)

✓ Δικαίωμα καταγγελίας

4. Κώδικες δεοντολογίας (Άρ. 40 & 41)

- «Φορείς ή ενώσεις που εκπροσωπούν υπεύθυνους ή εκτελούντες επεξεργασία **παροτρύνονται** να καταρτίζουν κώδικες δεοντολογίας»…

- «Κατά την κατάρτιση, διαβούλευση με την Αρχή και τα **ενδιαφερόμενα μέρη**»…

- **Παρακολούθηση εγκεκριμένων κωδίκων** (Άρ. 41, Παρ. 6)

  «Δεν εφαρμόζεται στην επεξεργασία από δημόσιες αρχές και φορείς» (?)

5. Εκτίμηση αντικτύπου (Αρ. 35/ΓΚ)

- «Απαιτείται στην επεξεργασία μεγάλης κλίμακας ειδικών κατηγοριών δεδομένων»..

  Κίνδυνος προερχόμενος από την επεξεργασία δεδομένων υγείας
- Δημοσιοποίηση καταλόγων με τα **είδη των πράξεων** που απαιτούν ή δεν απαιτούν εκτίμηση αντικτύπου
- Καταγραφή **πράξεων και σκοπών επεξεργασίας**
- **Εκτίμηση αναγκαιότητας και αναλογικότητας** πράξεων
- **Εκτίμηση κινδύνων για δικαιώματα και ελευθερία υποκειμένων**
- **Μέτρα – εγγυήσεις – μηχανισμοί ασφάλειας – απόδειξη συμμόρφωσης**

Ειδικά προβλήματα:

- Εκτίμηση **αξίας και ιδιοκτησίας δεδομένων Υγείας**
- Εκτίμηση **κινδύνου εμπορευματοποίησης**

6. Πιστοποίηση/Φορείς πιστοποίησης και διαπίστευσης

- Θέσπιση **μηχανισμών πιστοποίησης προστασίας δεδομένων**, (αιτ. σκ. 91)

«Η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν θα πρέπει να θεωρείται ότι είναι μεγάλης κλίμακας, εάν αφορά ΔΠΧ ασθενών ή πελατών ιδιώτη ιατρού, άλλου επαγγελματία υγείας, ή δικηγόρου. Στις περιπτώσεις αυτές, η εκτίμηση αντικτύπου της προστασίας δεδομένων δεν θα πρέπει να είναι υποχρεωτική».

(εξαίρεση μικρές – πολύ μικρές και μεσαίες επιχειρήσεις)

Φορείς πιστοποίησης:

Διαθέτουν διαπίστευση είτε από την Εποπτική Αρχή, είτε από τον Εθνικό Οργανισμό Διαπίστευσης (ΕΣΥΔ), σύμφωνα με το πρότυπο **EN – ISO/IEC 17065/2012**

IV. ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ

1. Αναγκαιότητα **«τομεακής» ρύθμισης** για την επεξεργασία των δεδομένων Υγείας
2. Συγκεκριμένες **υποχρεώσεις υπευθύνων επεξεργασίας και διοικήσεων ΕΟΠΥΥ - ΗΔΙΚΑ - Νοσοκομείων – Μονάδων Υγείας – Πολυιατρείων** δημόσιου και ιδιωτικού τομέα
3. Άμεση κάλυψη του **θεσμικού κενού** (Πρωτοβουλίες ΠΙΣ)
4. **Υποχρεώσεις εκτελούντων επεξεργασία:**

Ιατρικό σώμα, άλλοι επαγγελματίες υγείας, **συμβάσεις μεταξύ υπευθύνων και εκτελούντων**

IV. ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ

5. **Ευθύνες και μέτρα** σε περίπτωση παραβιάσεων ή μη τήρησης υποχρεώσεων συμμόρφωσης
6. **Ενημέρωση – εκπαίδευση** ιατρικού σώματος και **κατοχύρωση δικαιωμάτων ιατρών/επαγγελματιών Υγείας ως εργαζομένων**
7. **Μέτρα προστασίας** ιατρικού σώματος από την **εμπορευματοποίηση των πιστοποιήσεων**

ΠΡΟΕΤΟΙΜΑΣΙΑ ΓΙΑ ΤΟΝ GDPR ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ ΑΠΔΠΧ

ΕΝΗΜΕΡΩΣΗ - ΕΤΟΙΜΟΤΗΤΑ:

- **Ενημέρωση του ανθρώπινου δυναμικού του οργανισμού για τις επερχόμενες μεταβολές**, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων.
- **Αξιολόγηση των πιθανών κινδύνων για τα προσωπικά δεδομένα που συλλέγονται και επεξεργάζονται.**
- **Διαμόρφωση στρατηγικής αντιμετώπισης των πιθανών κινδύνων με τεχνικά και οργανωτικά μέτρα**, αφού έχει ελεγχθεί η υφιστάμενη πολιτική ασφαλείας.

ΚΑΤΑΓΡΑΦΗ

Αν υπάρχει υποχρέωση τήρησης ειδικών αρχείων επεξεργασιών, πρέπει να καταγράφονται λεπτομερώς τα δεδομένα που τηρούνται και μεταβιβάζονται, οι επεξεργασίες που πραγματοποιούνται, ο σκοπός και η νομική βάση.

Δημιουργία κεντρικού χάρτη προσωπικών δεδομένων και ροών των δεδομένων (data mapping, data flow audit).

Τήρηση αρχείου δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων.

ΕΛΕΓΧΟΣ ΤΗΡΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ

Συνεχής εξέταση για το αν κατά την επεξεργασία των δεδομένων τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία και αν γίνονται σεβαστά τα δικαιώματα των υποκειμένων.

- **Αρχές επεξεργασίας**: Αρχή νομιμότητας, αρχή αντικειμενικότητας, αρχή διαφάνειας, αρχή του σκοπού, αρχή της ελαχιστοποίησης των δεδομένων, αρχή της ακρίβειας, αρχή του περιορισμού, αρχή της ακεραιότητας και εμπιστευτικότητας, αρχή της λογοδοσίας.
- **Νομιμοποιητική βάση επεξεργασίας**: Άρθρα 6 και 9.
- **Δικαιώματα των υποκειμένων**: Άρθρα 12, 13 & 14, ανακοινώσεις άρθρων 15-22 & 34.

ΕΛΕΓΧΟΣ ΣΥΓΚΑΤΑΘΕΣΗΣ

Αν η νομιμοποιητική βάση της επεξεργασίας είναι η συγκατάθεση (Αρ. 7):

Εξέταση των μεθόδων για εξασφάλιση συγκατάθεσης για <u>κάθε</u> επιδιωκόμενο σκοπό επεξεργασίας: συγκατάθεση των φυσικών προσώπων πριν την επεξεργασία για κάθε επιδιωκόμενο σκοπό επεξεργασίας ξεχωριστά (η συγκατάθεση πρέπει να είναι ελεύθερη, ρητή, συγκεκριμένη, για σαφώς προσδιορισμένο σκοπό και να έχει προέλθει με σαφή θετική ενέργεια, ενώ ο τρόπος απόσυρσης της είναι απλός).

ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ

Επικαιροποίηση των διαδικασιών για τον χειρισμό των αιτημάτων και την ικανοποίηση των δικαιωμάτων των πολιτών, ιδίως ως προς τη διαγραφή δεδομένων (δικαίωμα στη λήθη) ή την παροχή τους σε αναγνώσιμο ηλεκτρονικό μορφότυπο (φορητότητα δεδομένων).

Τα δικαιώματα των υποκειμένων των δεδομένων περιγράφονται στα Άρθρα 12, 13 & 14, ανακοινώσεις στα πλαίσια των άρθρων 15-22 & 34. Στον GDPR προβάλλεται η ενισχυμένη αρχή της διαφάνειας και της λογοδοσίας.

ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ – ΔΙΕΝΕΡΓΕΙΑ ΜΕΛΕΤΗΣ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ

Θα πρέπει να υπάρχει εκτίμηση – αξιολόγηση των πιθανοτήτων επέλευσης κινδύνων και των συνεπειών στα προσωπικά δεδομένα.

Η διενέργεια εκτίμησης αντικτύπου περιέχει τουλάχιστον: α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς, γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων.

ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ανάλογα με τη δραστηριότητα που ασκείται, εξετάζεται αν χρειάζεται να οριστεί «υπεύθυνος προστασίας δεδομένων».

Ο διορισμός ΥΠΔ είναι υποχρεωτικός όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα διενεργείται από δημόσια αρχή/φορέα, όταν απαιτείται συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή όταν διενεργείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων (πχ. δεδομένων υγείας).

Τα ελάχιστα καθήκοντα του ΥΠΔ είναι:

- Να ενημερώνει σχετικά με τις υποχρεώσεις και να παρακολουθεί τη συμμόρφωση με τον ΓΚΠΔ και άλλες διατάξεις περί προστασίας δεδομένων
- Να παρέχει συμβουλές για την εκτίμηση αντικτύπου και να παρακολουθεί την υλοποίησή της
- Να είναι το σημείο επαφής με την ΑΠΔΠΧ και τα φυσικά πρόσωπα.

Ο ρόλος του ΥΠΔ είναι συμβουλευτικός και δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό.

ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ

- Υιοθέτηση μεθόδων για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων.
- Υιοθέτηση διαδικασίας για τις γνωστοποιήσεις παραβιάσεων προς την Αρχή και τα υποκείμενα;

ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΕΚΤΟΣ ΕΕ

Αν διαβιβάζονται δεδομένα και σε τρίτες χώρες, πρέπει να επιλεγεί κάποιος μηχανισμός διαβίβασης, όπως δεσμευτικοί εταιρικοί κανόνες, τυποποιημένες συμβατικές ρήτρες, πιστοποιήσεις στο Privacy Shield (για τις ΗΠΑ).

Σας ευχαριστώ!