ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ

ΙΑΤΡΙΚΟΣ ΣΥΛΛΟΓΟΣ ΗΡΑΚΛΕΙΟΥ (Ν.Π.Δ.Δ.)
ΚΡΙΤΟΒΟΥΛΙΔΟΥ 19 712 01 ΗΡΑΚΛΕΙΟ
ΤΗΛ.: 2810 283385 -2810 330193, FAX : 2810 330194
Web: www.ish.gr, e-mail: info@ish.gr

Ηράκλειο, 02/05/2018

ΣΗΜΕΙΩΜΑ ΠΡΟΕΔΡΟΥ

«Ο Γενικός Κανονισμός Προστασίας Δεδομένων στην καθημερινότητα ενός γιατρού»

Αγαπητοί συνάδελφοι,

Η σύνοδος προέδρων των Ιατρικών Συλλόγων της Χώρας που έγινε το Σάββατο 28 Απριλίου 2018, είχε θέμα την ενημέρωση σχετικά με τον Γενικό Κανονισμό για την Προστασία Δεδομένων - ΓΚΠΔ (General Data Protection Regulation – GDPR) και τι συνεπάγεται η εφαρμογή του στην επαγγελματική συμπεριφορά κάθε ιατρού. Από την 25η Μαΐου 2018 καθιερώνεται ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ. Ο Κανονισμός 2016/679, γνωστός ως **Γενικός Κανονισμός για την Προστασία Δεδομένων - ΓΚΠΔ (General Data Protection Regulation - GDPR)**, ψηφίστηκε πριν δύο χρόνια (Απρίλιος 2016). Με την εφαρμογή του:

- **Ενδυναμώνονται** τα δικαιώματα των φυσικών προσώπων ως προς την **ενημέρωση, την πρόσβαση, την διόρθωση** των προσωπικών τους δεδομένων**, τον περιορισμό** της επεξεργασίας τους, **την εναντίωσης** στην επεξεργασία αυτών, **την διαγραφή, την μεταφορά** και **την αποστολή** των προσωπικών του δεδομένων.

- **Αυξάνονται** οι υποχρεώσεις των υπεύθυνων της επεξεργασίας των δεδομένων. Με άξονες την **διαφάνεια και την λογοδοσία** ο υπεύθυνος επεξεργασίας έχει την **ευθύνη** συμμόρφωσης και απόδειξης ορθής τήρησης της διαδικασίας επεξεργασίας. Επιβάλλει επίσης, **την προστασία δεδομένων κατά τον σχεδιασμό** (χρήση- επιλογή προγραμμάτων με ρυθμίσεις αυξημένης προστασίας και ασφάλειας), **την προστασία δεδομένων εξ ορισμού** (τεχνικά μέτρα και προγράμματα επεξεργασίας μόνο των δεδομένων απαραίτητων για τον σκοπό της επεξεργασίας), **την ασφάλεια επεξεργασία**ς (εφαρμογή τεχνικών ρυθμίσεων- πρωτόκολλο ασφαλείας στα ήδη υπάρχοντα προγράμματα) **την γνωστοποίηση διαρροής δεδομένων** (από την στιγμή που θα γίνει αντιληπτή και εντός 72 ωρών στην αρχή προστασίας) **και τον Υπεύθυνο Προστασίας Δεδομένων (DPO)**. Ο DPO αποτελεί υποχρέωση σε όλα τα ΝΠΔΔ που επεξεργάζονται προσωπικά δεδομένα και όπου διενεργείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων.

Ως αποτέλεσμα όλων αυτών **ενισχύεται** η προστασία των προσωπικών δεδομένων.

Σύμφωνα με τον Κώδικα Ιατρικής Δεοντολογίας, ο ιατρός έχει την υποχρέωση να τηρεί ιατρικό αρχείο, σε ηλεκτρονική ή χειρόγραφη μορφή. Το ιατρικό αρχείο περιέχει δημογραφικά στοιχεία και το ιατρικό ιστορικό (ονοματεπώνυμο, πατρώνυμο, φύλο, ηλικία, επάγγελμα, διεύθυνση ασθενή, ημερομηνία επίσκεψης, καθώς και δεδομένα που συνδέονται με την ασθένεια, την υγεία του, την διάγνωση, τα αποτελέσματα εξετάσεων, την θεραπεία). Με τον όρο **επεξεργασία δεδομένων** εννοείται κάθε πράξη που πραγματοποιείται (ηλεκτρονικά ή χειρόγραφα) σε προσωπικά και ευαίσθητα δεδομένα. Η συλλογή, η οργάνωση, η χρήση, η αποθήκευση ακόμα και η διαγραφή προσωπικών δεδομένων ασθενών από οποιοδήποτε επαγγελματία υγείας θεωρείται επεξεργασία δεδομένων.

Με τον ΓΚΠΔ ενισχύονται σημαντικά τα δικαιώματα των ασθενών σχετικά με τα προσωπικά τους δεδομένα. Είναι προφανές ότι αυξάνονται οι υποχρεώσεις των ιατρών ως υπευθύνων επεξεργασίας, οι οποίοι επιφορτίζονται με την **αρχή της λογοδοσίας** (άρθρο 5). Η αρχή της λογοδοσίας αναλύεται σε επιμέρους ενέργειες που πρέπει να πραγματοποιεί ο γιατρός, ο οποίος ως υπεύθυνος επεξεργασίας, **φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση του** με τις γενικές αρχές που προβλέπει ο ΓΚΠΔ. Ας δούμε μερικά πρακτικά θέματα που προκύπτουν από την εφαρμογή του στην καθημερινή επαγγελματική δραστηριότητα του ιατρού:

- Όταν **η επεξεργασία βασίζεται στην συγκατάθεση**, ο υπεύθυνος πρέπει να μπορεί να αποδείξει την συγκατάθεση (χειρόγραφα ή ηλεκτρονικά, e-mail) (άρθρο 7)

- Προβλέπεται **η υποχρέωση του γιατρού να παρέχει στον ασθενή γραπτώς ή και ηλεκτρονικά τις πληροφορίες που αφορούν επεξεργασία των δεδομένων τους** (άρθρο 12). Για την ελαχιστοποίηση του λάθους στην αποστολή των δεδομένων ηλεκτρονικά, ζητήστε από τον ασθενή σας να αποστείλει πρώτος ηλεκτρονικό μήνυμα έτσι ώστε να ακολουθεί η δική σας απάντηση ως απαντητικό μήνυμα.

- Προβλέπεται **η υποχρέωση χορήγησης αντιγράφου** των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, όταν ο ασθενής το ζητήσει από τον γιατρό του (άρθρο 15).

Η αρχή της λογοδοσίας **αφορά και τον εκτελούντα την επεξεργασία**, ο οποίος επιλέγεται από τον υπεύθυνο επεξεργασίας. Η επεξεργασία διενεργείται κατόπιν γραπτής σύμβασης δεσμευτικής για τον εκτελούντα, ο οποίος επεξεργάζεται τα δεδομένα μόνο σύμφωνα με τις καταγεγραμμένες εντολές του υπευθύνου επεξεργασίας (άρθρο 28).

- Προβλέπεται ο γιατρός ως υπεύθυνος επεξεργασίας αλλά και ο εκτελών την επεξεργασία να τηρεί **αρχείο δραστηριοτήτων επεξεργασίας** (άρθρο 30). Στο αρχείο αυτό καταγράφει ενδελεχώς τα δεδομένα που τηρεί και μεταβιβάζει, τις επεξεργασίες στις οποίες προβαίνει, τον σκοπό και τη νομική βάση αυτών. Το αρχείο αυτό πρέπει να είναι πάντα στην διάθεση της Εποπτικής Αρχής όταν το ζητήσει.

- Προβλέπεται **η γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα** (άρθρο 33). **Εντός 72 ωρών** από την στιγμή που ο γιατρός αντιλαμβάνεται την παραβίαση οφείλει να την γνωστοποιήσει, αναλυτικά, αιτιολογημένα και τεκμηριωμένα, στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Ορισμός Υπεύθυνος Προστασίας Δεδομένων (DPO). Αποτελεί υποχρέωση όλων των ΝΠΔΔ που επεξεργάζονται προσωπικά δεδομένα και όπου διενεργείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων. Έχει την ευθύνη της παρακολούθησης της συμμόρφωσης και των πολιτικών προστασίας προσωπικών δεδομένων του υπευθύνου ή εκτελούντος την επεξεργασία. (άρθρο 39).

- **Η επεξεργασία δεδομένων προσωπικού χαρακτήρα ασθενών σε ιατρεία, όπου σχέση ιατρού – ασθενή είναι προσωπική,** δεν θεωρείται ότι είναι μεγάλης κλίμακας, επομένως δεν χρειάζεται D.P.O.

- **Σε κλινικές και νοσοκομεία** αποτελεί υποχρέωση ο ορισμός D.P.O

- Σε ενδιάμεσες περιπτώσεις **πολυιατρεία ή διαγνωστικά εργαστήρια** είναι απαραίτητη νομική συμβουλή για την αξιολόγηση του όγκου επεξεργασίας και δεδομένων.

Με βάση τον Κανονισμό αλλά και τις εισηγήσεις των ομιλητών κατά την ενημέρωση στη σύνοδο προέδρων:

- Η πιστοποίηση προστασίας δεδομένων έχει θέση ως **απόδειξη της συμμόρφωσης** προς τον Κανονισμό ή ως **απόδειξη παροχής κατάλληλων εγγυήσεων** κατά την επεξεργασίας και **είναι απολύτως εθελοντική.**

- Ο γιατρός που χρησιμοποιεί ΜΟΝΟ **το πρόγραμμα της ηλεκτρονικής συνταγογράφησης (ΗΔΙΚΑ), το e-dapy (ΕΟΠΥΥ) ή και προγράμματα πολυιατρείων, νοσοκομείων ή κλινικών** είναι χρήστες του συστήματος. Επιβάλλεται ωστόσο να τηρούν τις αρχές του Κανονισμού κατά την εισαγωγή των ευαίσθητων προσωπικών δεδομένων των ασθενών στο σύστημα.

Ο ΓΚΠΔ έχει την βάση του στον προηγούμενο νόμο περι προστασίας προσωπικών δεδομένων (ν.2472/1997) . Επιγραμματικά με την εφαρμογή του:

1. **Οι ασθενείς** αποκτούν δικαίωμα στην ενημέρωση, στην πρόσβαση, στην διόρθωση, στον περιορισμό, στην εναντίωσης της επεξεργασίας στη λήθη και στη φορητότητα των δεδομένων τους.

2. Η **συναίνεση – ρητή συγκατάθεση** των ασθενών είναι απαραίτητη για την καταγραφή & διαχείριση των δεδομένων.

3. Για την κοινοποίηση – αποστολή προσωπικών δεδομένων σε τρίτους (ακόμα και άτομα της οικογένειας) απαιτείται **έγγραφη εξουσιοδότηση**. Στην ηλεκτρονική αποστολή ζητήστε από τον

ασθενή να αποστείλει πρώτος ηλεκτρονικό μήνυμα, ώστε να ακολουθεί η αποστολή σας ως απαντητικό μήνυμα.

4. **Όλοι οι γιατροί** (ελεύθεροι επαγγελματίες και στις μονάδες υγείας) με άξονες την διαφάνεια (τρόπος συλλογής, επεξεργασίας και τήρησης) και την λογοδοσία (συμμόρφωση - ορθή τήρηση διαδικασιών) είναι υπεύθυνοι για την τήρηση του.
5. Είναι απαραίτητη η ενημέρωση του προσωπικού που απασχολούνται στις μονάδες υγείας (γραμματείς, νοσηλευτές, παρασκευαστές) για τις αλλαγές που επιφέρει ο ΓΚΠΔ.
6. Είναι απαραίτητη η **τήρηση αρχείου δραστηριοτήτων επεξεργασίας.**
7. Αναθεώρηση πολιτικών προστασίας δεδομένων:

   - Επιλογή και χρήση προγραμμάτων με ρυθμίσεις αυξημένης προστασίας και ασφάλειας, με δυνατότητα πρόσβασης μόνο στα άτομα που εμπλέκονται στην επεξεργασία αυτών.

   - Εφαρμογή τεχνικών ρυθμίσεων και πρωτόκολλου ασφαλείας στα ήδη υπάρχοντα δεδομένα.

8. **Γνωστοποίηση διαρροής δεδομένων**. (από την στιγμή που θα γίνει αντιληπτό και εντός 72 ωρών στην αρχή προστασίας).
9. Ο **Υπεύθυνος Προστασίας Δεδομένων (DPO)** είναι υποχρεωτικός για όλα τα ΝΠΔΔ. **Για τα μεμονωμένα ιατρεία προαιρετικός, εξαρτάται από τον όγκο των δεδομένων.** Μπορεί να είναι ανεξάρτητος ή και υπάλληλος του οργανισμού. Παρακολουθεί, επιβλέπει, ενημερώνει, επικοινωνεί με την Αρχή.
10. **Η πιστοποίηση** είναι εθελοντική, αποτελεί **απόδειξη συμμόρφωσης** και δεν προστατεύει.

Είναι αυτονόητο ότι κάθε περίπτωση α**ξιολογείται ξεχωριστά** με βάση τα χαρακτηριστικά της (ιατρείο, πολυιατρείο, όγκος επεξεργασίας κτλ). **Ο ΓΚΠΔ ισχύει για όλους** ανεξάρτητα από την παρουσία υπευθύνου Προστασίας Δεδομένων (DPO).

Στο πλαίσιο της έγκυρης ενημέρωσης σχεδιάζουμε άμεσα ενημερωτική ημερίδα με στόχο να λυθεί κάθε απορία και προβληματισμός βοηθώντας ουσιαστικά στην προετοιμασία για την εφαρμογή του ΓΚΠΔ στην επαγγελματική μας καθημερινότητα.

Με εκτίμηση

Ο Πρόεδρος του ΙΣΗ

Χάρης Χ. Βαβουρανάκης