ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Eurobank

Secure HealthData

ΑΣΦΑΛΕΙΑ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΥΓΕΙΑ

"Ιδιωτικό ιατρείο στα χρόνια του GDPR"

Φελεκίδης Αναστάσιος

Ιατρός Οφθαλμίατρος, Ιατρικός Σύλλογος Ξάνθης

ΙΔΙΩΤΙΚΟ ΙΑΤΡΕΙΟ

ΣΤΑ ΧΡΟΝΙΑ ΤΟΥ GDPR

ΦΕΛΕΚΙΔΗΣ ΑΝΑΣΤΑΣΙΟΣ

ΟΡΙΣΜΟΣ

- **Προσωπικό δεδομένο θεωρείται κάθε πληροφορία σχετική με ένα φυσικό πρόσωπο, εφόσον αυτό το φυσικό πρόσωπο *ταυτοποιείται ή μπορεί να ταυτοποιηθεί* (δηλαδή ακόμη και εάν δεν προσδιορίζεται ΑΜΕΣΑ ποιο είναι το πρόσωπο που αφορά η πληροφορία, αλλά αυτό μπορεί να συναχθεί ΕΜΜΕΣΑ συνδυάζοντας άλλες πληροφορίες).**

τι κάνει ο GDPR

- **εξισορροπεί το δικαίωμα των ατόμων στην ιδιωτικότητα και την ανάγκη των οργανισμών και των επαγγελματιών να επεξεργάζονται δεδομένα για επαγγελματικούς σκοπούς.**
- **Υπεύθυνος επεξεργασίας –ιατρός**
- **Υποκείμενο δεδομένων – ασθενής**
- **Εκτελών την επεξεργασία-προσωπικό , συνεργάτες**

Δικαιώματα των Ασθενών

- • Δικαίωμα πρόσβασης - Δικαίωμα να λαμβάνει πληροφορίες για το εάν γίνεται επεξεργασία δεδομένων και δικαίωμα πρόσβασης σε αυτά. Δικαίωμα ενημέρωσης σχετικά με την επεξεργασία αυτή (ποιος, για ποιο σκοπό, παραλήπτες, περίοδος διατήρησης κ.λπ.)
- • Δικαίωμα στην διόρθωση - Δικαίωμα διόρθωσης ανακριβών προσωπικών δεδομένων και συμπλήρωσης ελλιπών πληροφοριών.
- • Δικαίωμα διαγραφής (Δικαίωμα στη λήθη) - Δικαίωμα να ζητείται η διαγραφή οποιωνδήποτε δεδομένων που αφορούν το / τα υποκείμενο υπό ορισμένες προϋποθέσεις (δεδομένα που δεν είναι πλέον απαραίτητα, ανάκληση συγκατάθεσης, δεδομένα που έχουν υποβληθεί σε παράνομη επεξεργασία).
- • Δικαίωμα Περιορισμού της Επεξεργασίας - όταν αμφισβητείται η ακρίβεια των δεδομένων, η επεξεργασία είναι παράνομη, τα δεδομένα δεν χρειάζονται πλέον στον υπεύθυνο επεξεργασίας, το υποκείμενο των δεδομένων έχει αντιταχθεί στην αυτοματοποιημένη επεξεργασία)
- • Δικαίωμα στη φορητότητα των δεδομένων - Δικαίωμα αίτησης διαβίβασης δεδομένων προσωπικού χαρακτήρα σε άλλον Υπεύθυνο Επεξεργασίας σε δομημένη, ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή.
- • Δικαίωμα ενημέρωσης κατά την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα και διατύπωση αντιρρήσεων όταν η απόφαση βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, και η απόφαση αυτή παράγει έννομα αποτελέσματα ή επηρεάζει σημαντικά το υποκείμενο των δεδομένων. Δικαίωμα να ζητείται η ανθρώπινη παρέμβαση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Παραβίαση δεδομένων προσωπικού χαρακτήρα

- Παραβίαση Εμπιστευτικότητας
- Παραβίαση Ακεραιότητας
- Παραβίαση Διαθεσιμότητας

GDPR ΓΙΑ ΟΛΟΥΣ

Ο ΙΑΤΡΟΣ ΥΠΟΧΡΕΩΤΙΚΑ

Διαθέτει έντυπο ενημέρωσης και λαμβάνει συναίνεση των ασθενών του εάν πρόκειται να κάνει χρήση δεδομένων και για άλλους σκοπούς πέραν της τήρησης ιατρικού αρχείου: Εάν τα προσωπικά δεδομένα των ασθενών πρόκειται να χρησιμοποιηθούν και για άλλους σκοπούς (π.χ. αποστολή μηνύματος για υπενθύμιση επανελέγχου, τηλεφωνική κλήση για ραντεβού, χρήση στοιχείων για κλινική έρευνα, παροχή στοιχείων ασθενών σε τρίτους για άλλους σκοπούς), τότε ο ιατρός οφείλει:

α) να ενημερώσει με σαφήνεια τον ασθενή για την περαιτέρω χρήση των δεδομένων του και για το σκοπό αυτής και

β) να μην προχωρήσει στην περαιτέρω χρήση τους αν δεν λάβει τη συναίνεση του ασθενούς για κάθε σκοπό ξεχωριστά.

Πρέπει να τηρώ Αρχείο Δραστηριοτήτων Επεξεργασίας

- **Το άρθρο 30 προβλέπει την υποχρέωση του Υπεύθυνου Επεξεργασίας να τηρεί ένα αρχείο όπου καταγράφονται οι δραστηριότητες επεξεργασίας για τις οποίες είναι υπεύθυνος. Το αρχείο πρέπει να περιλαμβάνει:**
- **Όνομα και στοιχεία επικοινωνίας υπεύθυνου επεξεργασίας, εκπροσώπου και DPO (εάν έχει οριστεί)**
- **Σκοπούς επεξεργασίας**
- **Κατηγορίες υποκειμένων δεδομένων (π.χ. ασθενείς, εργαζόμενοι)**
- **Κατηγορίες αποδεκτών στους οποίους γνωστοποιούνται τα δεδομένα**
- **Διαβιβάσεις σε τρίτες χώρες ή διεθνείς οργανισμούς**
- **Προβλεπόμενες προθεσμίες διαγραφής**
- **Τεχνικά και οργανωτικά μέτρα ασφάλειας**

Πρέπει να τηρώ Αρχείο Δραστηριοτήτων Επεξεργασίας

- **Στην παράγραφο 5 προβλέπεται παρέκλιση από αυτήν την υποχρεώση για επιχειρήσεις ή οργανισμούς που απασχολούν λιγότερο από 250 άτομα. Ωστόσο, η παρέκκλιση που προβλέπεται στο άρθρο 30 παράγραφος 5 δεν είναι απόλυτη.**
- **Όταν γίνεται επεξεργασία δεδομένων υγείας, που εμπίπτουν στην κατηγορία των ειδικών κατηγοριών δεδομένων, δεν ισχύει η παρέκλιση. Επιβάλλεται η τήρηση αρχείου επεξεργασίας, ακόμη και εάν ο υπεύθυνος επεξεργασίας απασχολεί λιγότερα από 250 άτομα.**

Αρχείο Επεξεργασίας του GDPR και Ιατρικό Αρχείο

- **Στο Αρχείο Επεξεργασίας του GDPR καταγράφουμε διαδικασίες. Δεν καταγράφουμε στοιχεία συγκεκριμένων ασθενών. Δεν χρειάζεται να παρέχεται στους ασθενείς. Ο ιατρός το τηρεί για δική του χρήση στο ιατρείο για την καλύτερη οργάνωσή του ή/και για τυχόν έλεγχο από Αρχές.**
- **Τα στοιχεία ασθενών εξακολουθούν να καταγράφονται στο Ιατρικό Αρχείο, όπως αυτό προβλέπεται από το Άρθρο 14 του Κώδικα Ιατρικής Δεοντολογίας. Η δομή και το περιεχόμενο του Ιατρικού Αρχείου με τα στοιχεία των ασθενών δεν τροποποιείται από τις διατάξεις του GDPR ούτε αντικαθίσταται από κάποιο άλλο αρχείο.**

Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO)

- Υπευθυνος για την προστασία των δεδομένων ώστε να διασφαλίζεται η συμμόρφωση με την ισχύουσα νομοθεσία
- Ωστόσο, η επεξεργασία δεδομένων υγείας που πραγματοποιείται από ιδιώτη ιατρό δεν συνιστά μεγάλης κλίμακας επεξεργασία και ως εκ τούτου στην περίπτωση αυτή δεν είναι υποχρεωτικός ο ορισμός Υπεύθυνου Προστασίας Δεδομένων
- Σε ενδιάμεσες κατηγορίες, το εάν ο ορισμός Υπεύθυνου Προστασίας δεδομένων είναι υποχρεωτικός ή όχι, θα πρέπει να κρίνεται κατά περίπτωση με τη συνδρομή εξειδικευμένων νομικών

Προσωπικό

- **Συμμόρφωση με κανονισμό**
- **Σε υπηρεσία τηλεφωνικής γραμματείας, σύμβαση με την εταιρεία που παρέχει την τηλεφωνική γραμματεία και να προβλεφθεί ότι η εταιρεία που συλλέγει για λογαριασμό σας τα στοιχεία των ασθενών που κλείνουν ραντεβού αναλαμβάνει τις υποχρεώσεις της ως εκτελούσα την επεξεργασία.**

Αποτελέσματα ιατρικών εξετάσεων σε τρίτους

- Τα αποτελέσματα εξετάσεων αποτελούν προσωπικά δεδομένα, επομένως πρέπει να τα διασφαλίσετε .Ύπαρξη έντυπου, το οποίο θα συμπληρώνει κάθε ασθενής πριν εξεταστεί και στο οποίο, θα περιλαμβάνει και ένα πεδίο που θα συμπληρώνεται υποχρεωτικά και όπου ο ασθενής θα δηλώνει με ποιον τρόπο θα παραλάβει τα αποτελέσματα των εξετάσεών του. Σε περίπτωση που ο ασθενής δηλώσει ότι επιθυμεί να παραλάβει τα αποτελέσματα τρίτος, θα πρέπει (ο ασθενής) να συμπληρώσει το πλήρες ονοματεπώνυμο του τρίτου (συνιστάται να αναφέρεται και ο αριθμός ταυτότητας) και να υπογράψει το έντυπο. Κατά την παράδοση των αποτελεσμάτων των εξετάσεων στον τρίτο, πρέπει να ελέγχεται η ταυτοπροσωπία

Διενέργεια εξετάσεων από συνεργάτη & ενημέρωση ασθενούς

- **Ο ασθενής θα πρέπει να ενημερώνεται σχετικά με το εάν τα δεδομένα του θα διαβιβαστούν σε τρίτους αποδέκτες. Δεν χρειάζεται αρχικά να προσδιοριστούν ακριβώς οι τρίτοι (π.χ. στο Χ εργαστήριο) αλλά οι κατηγορίες τους (π.χ. "σε ορισμένες περιπτώσεις τα στοιχεία σας και το βιολογικό υλικό αποστέλλονται σε συνεργαζόμενα εργαστήρια για την ολοκλήρωση των εξετάσεων"). Εάν ο ασθενής ασκήσει το δικαίωμα πρόσβασης, δικαιούται να ενημερωθεί με μεγαλύτερη λεπτομέρεια σχετικά με τους αποδέκτες των δεδομένων του. Στην περίπτωση αυτή θα πρέπει εντός 1 μηνός να του παράσχετε όλα τα αναγκαία στοιχεία, συμπεριλαμβανομένων των στοιχείων των αποδεκτών – συνεργατών σας.**

Συνεργάτες ιατρείου και απόρρητο ασθενών

- **Εάν οι συνεργάτες σας είναι άλλοι ιατροί, δεσμεύονται από το νόμο για την τήρηση του ιατρικού απορρήτου, επομένως αυτή η δέσμευση ισχύει ακόμη και εάν δεν υπογράψουν κάποιο κείμενο που τους δεσμεύει ειδικά.**
- **Εργαζόμενοί όπως γραμματείς, που δεν δεσμεύονται από το ιατρικό απόρρητο από το νόμο, θα πρέπει στη σύμβασή τους ή/και σε χωριστό έγγραφο να αναλάβουν την «υποχρέωση να τηρούν την εμπιστευτικότητα των δεδομένων των ασθενών και να συμμορφώνονται με το πλαίσιο που διέπει την προστασία προσωπικών δεδομένων». Το κείμενο αυτό μπορεί να εμπλουτίζεται κατά περίπτωση με ειδικότερες προβλέψεις (π.χ. εάν έχετε καταγράψει βασικούς κανόνες ασφάλειας για τη χρήση ηλεκτρονικού υπολογιστή, να αναφέρετε στη σύμβαση/δήλωση ότι θα τηρούν πάντοτε αυτούς τους κανόνες).**

Συστήματα Πληροφορικής

- **Χρήση λογισμικού**
- **Υποχρέωση εταιρειών**
- **Κανόνες ασφάλειας**

τεχνικά μέτρα ασφαλείας

- ισχυρό - δύσκολο password ανά τακτά χρονικά διαστήματα αλλαγή
- Απενεργοποίηση λειτουργίας μέσων αποθήκευσης (π.χ. USB) όπου αυτή δεν χρειάζεται (π.χ. PC γραμματείας).
- Χρήση μοντέρνων λειτουργικών συστημάτων υπολογιστή και συνεχόμενη ενημέρωσή τους.
- Χρήση λογισμικού προστασίας από κακόβουλο λογισμικό (antivirus) και Τείχους Προστασίας (Firewall) στον υπολογιστή.
- Αποφυγή χρήσης λογισμικού ελεύθερης χρήσης (free download).
- Αποφυγή χρήσης και παραχώρησης προνομιακών δικαιωμάτων πρόσβασης στον απλό χρήστη (δικαιώματα Local Administrator).
- Λήψη αντιγράφων ασφάλειας σε τακτά χρονικά διαστήματα.
- Αποφυγή χρήσης ελευθέρων e-mail, π.χ. Yahoo, για αποστολή και λήψη ευαίσθητων δεδομένων, π.χ. ιατρικών εξετάσεων.
- Κρυπτογράφηση τοπικού δίσκου υπολογιστή μέσω του λειτουργικού συστήματος.
- Κρυπτογράφηση εξωτερικών μονάδων αποθήκευσης (π.χ. εξωτερικός σκληρός δίσκος, USB κ.ο.κ.).

ΕΥΧΑΡΙΣΤΩ