Προστασία Προσωπικών Δεδομένων σε Ιδιωτικά Ιατρεία / Πολυιατρεία

Δημοσθένης Κ. Κωστούλας MBA, MSc, BSc

Υπεύθυνος Προστασίας Δεδομένων (DPO) Ιατρικού Συλλόγου Θεσσαλονίκης, dpo@isth.gr

Για τα ιδιωτικά ιατρεία / πολυιατρεία (ως φορείς παροχής υπηρεσιών πρωτοβάθμιας περίθαλψης), αν και δεν απαιτείται ο διορισμός υπεύθυνου προστασίας δεδομένων, αφού δεν λαμβάνει χώρα μεγάλης κλίμακας επεξεργασία δεδομένων, κρίνεται επιτακτική μια σειρά από κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων ασθενών, προσωπικού κλπ. Αν και η έκταση και το εύρος εφαρμογής αυτών των μέτρων μπορεί να διαφοροποιούνται, **συστήνεται η υλοποίηση μιας – κατ΄ελάχιστον – λίστας προληπτικών ενεργειών.**

Ενδεικτικά, αλλά όχι περιοριστικά:

- Δημιουργία ενός αρχείου δραστηριοτήτων με όλες τις κατηγορίες επεξεργασίας των προσωπικών δεδομένων για τις οποίες είναι υπεύθυνος ο Ιατρός (ως υπεύθυνος επεξεργασίας), με ταυτόχρονη αναφορά σε μια σειρά από βασικές πληροφορίες που απαιτούνται από τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ ή GDPR).
- Ιδεατά, ύπαρξη μιας πολιτικής προστασίας δεδομένων προσωπικού χαρακτήρα.
- Ύπαρξη κατάλληλου εντύπου ενημέρωσης των πελατών / ασθενών για την χρήση των δεδομένων τους, με αναφορά στους σκοπούς για τους οποίους που θα χρησιμοποιηθούν τα δεδομένα, την νομική βάση για την επεξεργασία τους, για πόσο χρονικό διάστημα θα αποθηκεύονται, σε ποιους θα κοινοποιούνται, αναφορά στα βασικά δικαιώματά των ασθενών όσον αφορά την προστασία των δεδομένων τους, το δικαίωμά τους να υποβάλουν καταγγελία στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) κλπ.
- Σε περίπτωση απασχόλησης προσωπικού (π.χ. γραμματεία κλπ.), ύπαρξη εντύπου ενημέρωσης του προσωπικού για τις ακριβείς επεξεργασίες των προσωπικών του δεδομένων και, ξεχωριστά, υπογραφή ρήτρας εμπιστευτικότητας. Επίσης, συχνή εκπαίδευση του προσωπικού για την ορθολογική χρήση των υπηρεσιακών δεδομένων (σε φυσική ή/και ηλεκτρονική μορφή).
- Στην περίπτωση των προμηθευτών και των εξωτερικών συνεργατών, απαίτηση για υπογραφή σύμβασης ή άλλης νομικής πράξης σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, κατά περίπτωση και βάση του είδους της εκάστοτε συνεργασίας. Ενδεικτικά, μπορεί να αφορά την ανάθεση σε τρίτες εταιρείες ή ελεύθερους επαγγελματίες της λογιστικής ή/και μηχανογραφικής υποστήριξης του ιατρείου, της διαχείρισης της ιστοσελίδας ή/και των λογαριασμών κοινωνικής δικτύωσης του ιατρείου, της καθαριότητας ή/και φύλαξης του ιατρείου κλπ. Επιπλέον, απαιτείται η υπογραφή σύμβασης στην περίπτωση διαβίβασης δεδομένων ή/και βιολογικών δειγμάτων ασθενών σε συνεργαζόμενα εργαστήρια ή άλλες μονάδες παροχής υπηρεσιών υγείας.
- Σε περίπτωση λειτουργίας κλειστού κυκλώματος τηλεόρασης (CCTV), α) ενημέρωση των ασθενών και επισκεπτών με εμφανείς σημάνσεις για την ύπαρξη του συστήματος βιντεοεπιτήρησης για το σκοπό της ασφάλειας προσώπων και αγαθών και β) τήρηση των σχετικών απαιτήσεων που

προκύπτουν από την κείμενη νομοθεσία (,ενδεικτικά, τοποθέτηση καμερών σε σημεία εισόδου και εξόδου και όχι σε χώρους αναμονής).

- Σε περίπτωση ύπαρξης ηλεκτρονικής ιστοσελίδας, ύπαρξη όρων και προϋποθέσεων χρήσης της ιστοσελίδας, δυνατότητα στον επισκέπτη να αποδεχθεί ή να απορρίψει την εγκατάσταση cookies (πέραν των «αυστηρώς απαραίτητων»), ανάρτηση στην ιστοσελίδα της πολιτικής προστασίας δεδομένων κλπ.
- Σε περίπτωση αποστολής ηλεκτρονικών newsletters ή SMS marketing, θα πρέπει οπωσδήποτε να δίδεται η δυνατότητα στους χρήστες για ξεκάθαρη και ρητή συγκατάθεση για το αν επιθυμούν να λαμβάνουν τέτοιες επικοινωνίες / ενημερώσεις (opt-in).
-

Ειδικότερα ως προς **την φυσική ασφάλεια**, προτείνονται ενδεικτικά τα ακόλουθα μέτρα:

- ασφαλής αποθήκευση κρίσιμων δεδομένων, όπως φύλαξη φακέλων προσωπικού, ασθενών και λοιπά έντυπα αρχεία σε κλειδωμένα συρτάρια, ντουλάπες ή φωριαμούς,
- ιδεατά, εγκατάσταση συστήματος συναγερμού και αλλαγή κωδικών σε περίπτωση αποχώρησης προσωπικού που τους γνώριζε,
- ιδεατά, εγκατάσταση κλειστού κυκλώματος τηλεόρασης (CCTV),

αλλαγή κλειδαριών σε περίπτωση αποχώρησης προσωπικού που χειριζόταν τα κλειδιά, κλείδωμα όλων των θυρών και παραθύρων του ιατρείου πριν την αποχώρηση κλπ.

Ως προς την **ασφάλεια της ηλεκτρονικής πληροφορίας**, προτείνονται ενδεικτικά τα ακόλουθα μέτρα:

- εφαρμογή προγραμμάτων αντιμετώπισης κακόβουλου λογισμικού (anti malware), καθώς και χρήση προγραμμάτων τειχών ασφαλείας (firewall),
- αποθήκευση στο δίκτυο και κεντρική λήψη αντιγράφων ασφαλείας (backup), σε τακτική βάση και με ασφαλή τρόπο,
- περιορισμοί στην σύνδεση αποσπώμενων μέσων για αποφυγή κακόβουλης εξαγωγής δεδομένων,
- διαχείριση λογαριασμών χρηστών, μηχανισμοί ελέγχου πρόσβασης, διαχείριση κωδικών πρόσβασης,
- λοιπές διαδικασίες για την προστασία της ηλεκτρονικής πληροφορίας και δεδομένων.

Ως προς τις **διαβιβάσεις πληροφοριών**, προτείνονται ενδεικτικά τα ακόλουθα μέτρα:

- προστασία ηλεκτρονικών αρχείων κατα την αποστολή τους μέσω ηλεκτρονικού ταχυδρομείου (πχ μέσω της ξεχωριστής αποστολής των κωδικών ανοίγματος με SMS ή με άλλους ενδεδειγμένους τρόπους προστασίας),
- διαδικασίες για προσεκτική ταυτοποίηση ατόμων πριν την διαβίβαση πληροφοριών δια τηλεφώνου, ηλεκτρονικά ή από κοντά κλπ.

Στην περίπτωση επεξεργασίας δεδομένων για πιο ειδικούς σκοπούς, όπως για παράδειγμα, διαβίβαση δεδομένων ασθενή σε ασφαλιστική εταιρία, σε άλλους ιατρούς για λήψη δεύτερης γνώμης, επεξεργασία για σκοπούς επιστημονικής έρευνας,

επεξεργασία στο πλαίσιο κλινικών δοκιμών κλπ., θα πρέπει πάντα να εξετάζεται προσεκτικά ποιος είναι ο σκοπός και η ενδεδειγμένη νομική βάση, παράλληλα με την τήρηση όλων των απαραίτητων μέτρων προστασίας.

Συμπερασματικά, τα ιδιωτικά ιατρεία / πολυιατρεία, ως φορείς παροχής υπηρεσιών πρωτοβάθμιας υγείας, δεν θα πρέπει απλώς να αντιλαμβάνονται τον σκοπό και την σημαντικότητα της προστασίας των δεδομένων προσωπικού χαρακτήρα που διαχειρίζονται, αλλά και να υιοθετούν μια σειρά από τεχνικά και οργανωτικά μέτρα προστασίας και διαφύλαξης των δεδομένων, υπό το πρίσμα του ΓΚΠΔ / GDPR και της κείμενης νομοθεσίας.

Έντυπο ενημέρωσης ασθενή – Γενικό Υπόδειγμα
https://isth.gr/wp-content/uploads/2023/04/Εντυπο-ενημέρωσης-ασθενή-σε-ιδιωτικό-ιατρείο-Γενικό-υπόδειγμα.pdf

Έντυπο ενημέρωσης ασθενή προς υπογραφή από τον ασθενή:
https://isth.gr/wp-content/uploads/2023/04/Εντυπο-ενημέρωσης-ασθενή-σε-ιδιωτικό-ιατρείο-με-υπογραφή.pdf