Προστασία Προσωπικών Δεδομένων σε Φορείς Παροχής Πρωτοβάθμιας Περίθαλψης (ιδιωτικά ιατρεία / πολυιατρεία)

Δημοσθένης Κ. Κωστούλας, Υπεύθυνος Προστασίας Δεδομένων (DPO) του Ιατρικού Συλλόγου Θεσσαλονίκης, ***dpo@isth.gr***

Για τους φορείς παροχής υπηρεσιών πρωτοβάθμιας περίθαλψης (ιδιωτικά ιατρεία / πολυιατρεία), αν και δεν απαιτείται ο διορισμός υπεύθυνου προστασίας δεδομένων (DPO), αφού δεν λαμβάνει χώρα μεγάλης κλίμακας επεξεργασία δεδομένων, ένα ιδιωτικό ιατρείο / πολυιατρείο οφείλει να εφαρμόσει μια σειρά από κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων. 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 υπεύθυνο το ιατρείο (ως υπεύθυνος επεξεργασίας), με ταυτόχρονη αναφορά σε μια σειρά από βασικές πληροφορίες που απαιτούνται από τον Γενικό Κανονισμό Προστασίας Δεδομενων (ΓΚΠΔ / GDPR) και την κείμενη νομοθεσία.
- Ύπαρξη μιας πολιτικής προστασίας δεδομένων προσωπικού χαρακτήρα.
- Ορισμένες γραπτές διαδικασίες για τον τρόπο επεξεργασίας των προσωπικών δεδομένων από το ιατρείο / τον ιατρό.
- Ύπαρξη κατάλληλου εντύπου ενημέρωσης των 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, το δικαίωμά τους να υποβάλουν καταγγελία κλπ.

- Σε περίπτωση απασχόλησης προσωπικού (γραμματεία κλπ.), ύπαρξη εντύπου ενημέρωσης του προσωπικού για τις ακριβείς επεξεργασίες των προσωπικών τους δεδομένων και, ξεχωριστά, υπογραφή ρήτρας εμπιστευτικότητας. Επίσης, συχνή εκπαίδευση του προσωπικού για την ορθολογική χρήση των υπηρεσιακών δεδομένων (σε κάθε 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 συνεργασίας. Ενδεικτικά, αφορά την ανάθεση σε τρίτες εταιρείες ή ελεύθερους επαγγελματίες: α) της μισθοδοσίας του προσωπικού, β) της ασφάλισης του προσωπικού, γ) της λογιστικής υποστήριξης του ιατρείου, δ) της μηχανογραφικής υποστήριξης, ε) της διαχείρισης της εταιρικής ιστοσελίδας ή/και των social media, στ) της συντήρησης του εξοπλισμού, ζ) της καθαριότητας των υποδομών, η) της φύλαξης των υποδομών και θ) τυχών λοιπές συνεργασίες με συμβούλους. Επιπλέον, απαιτούνται συμβάσεις με τυχόν συνεργαζόμενα εργαστήρια ή με 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, όπως ενδεικτικά, τοποθέτηση καμερών σε σημεία εισόδου και εξόδου, σε χώρους ταμείων ή χώρους

κρίσιμων εγκαταστάσεων, απαίτηση για διαγραφή του καταγεγραμμένου υλικού εντός 15 ημερών, προστασία μονάδας ελέγχου του κυκλώματος (καταγραφικό) το υλικό να μην χρησιμοποιείται για την διαδικασία αξιολόγησης του προσωπικού κλπ.

- 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,
- εγκατάσταση συστήματος συναγερμού και αλλαγή κωδικών σε περίπτωση αποχώρησης προσωπικού που τους γνώριζε,
- εγκατάσταση κλειστού κυκλώματος τηλεόρασης (CCTV) ή/και συνεργασία με εταιρεία φύλαξης χώρων (security),
- αλλαγή κλειδαριών σε περίπτωση αποχώρησης προσωπικού που χειριζόταν τα κλειδιά,
- κλείδωμα όλων των θυρών και παραθύρων 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 πολιτικές και 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),
- μηχανισμοί και διαδικασίες για προσεκτική ταυτοποίηση ατόμων πριν την διαβίβαση πληροφοριών δια τηλεφώνου, ηλεκτρονικά ή από κοντά κλπ.

Στην περίπτωση επεξεργασίας δεδομένων για τους ακόλουθους σκοπούς (ενδεικτικά), θα πρέπει πάντα **να εξετάζεται προσεκτικά ποιος είναι ο σκοπός και η ενδεδειγμένη νομική βάση**, παράλληλα με την τήρηση όλων των απαραίτητων μέτρων προστασίας:

- τηλεφωνικές επικοινωνίες από το ιατρείο προς τον ασθενή ή αποστολή μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου ή SMS, αποκλειστικά και μόνο για την ενημέρωση / παρακολούθηση της κατάστασής της υγείας του ή για

υπενθύμιση τυχόν περιοδικού ελέγχου ή επόμενης επίσκεψης (ενημέρωση ασθενή),

- αποστολή δεδομένων ασθενή (συνολικά ή μέρος αυτών, όπως κάθε φορά απαιτείται) σε συνεργαζόμενους ιατρούς για τη λήψη δεύτερης γνώμης, σε διαγνωστικά εργαστήρια ή /και σε λοιπούς παρόχους υπηρεσιών υγείας για την διενέργεια εξετάσεων που δεν πραγματοποιούνται στο ιατρείο ή/και για την καλύτερη παροχή υπηρεσιών υγείας (ενημέρωση ασθενή),
- διαβίβαση δεδομένων ασθενή στην ασφαλιστική εταιρία του ασθενή για αποζημίωση ιατρικών υπηρεσιών (συγκατάθεση από ασθενή),
- χρήση δεδομένων ασθενή σε επιστημονικές έρευνες στο πλαίσιο κλινικών δοκιμών (συγκατάθεση από ασθενή),
- λήψη φωτογραφιών για την παρακολούθηση της πορείας της υγείας του ασθενή (ενημέρωση ασθενή),
- ανάρτηση στο διαδίκτυο φωτογραφιών του ασθενή, με μέριμνα ώστε να μην αποκαλύπτεται άμεσα ή έμμεσα η ταυτότητά του ασθενή (συγκατάθεση από ασθενή) κλπ.

Συμπερασματικά, τα ιδιωτικά ιατρεία / πολυιατρεία και οι λοιποί 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 (Ν. 4624/2019).