ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΙΑΤΡΙΚΟΣ ΣΥΛΛΟΓΟΣ ΣΕΡΡΩΝ - Ν.Π.Δ.Δ.

ΤΣΑΛΟΠΟΥΛΟΥ 12 – ΣΕΡΡΕΣ – Τ.Κ. 62122

Τηλ: 23210 22202 - Fax: 23210 22910

e-mail: iatr-ser@otenet.gr

Σέρρες, Παρασκευή, 18 Μαΐου 2018

Α.Π:

Προς: Τα μέλη του Ιατρικού Συλλόγου Σερρών

Θέμα: Ενημέρωση για τον κανονισμό GDPR

Αγαπητοί συνάδελφοι

Όπως σας είχα υποσχεθεί στη συνάντησή μας στα γραφεία του Συλλόγου στις 2 Μαΐου 2018, σας μεταφέρω (έστω και καθυστερημένα) κάποιες πληροφορίες για τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR).

Αυτές προέρχονται κυρίως τις σημειώσεις που κράτησα και τις ερωτήσεις που υποβλήθηκαν κατά την ενημέρωση για το θέμα, που έγινε προς τους προέδρους των Ιατρικών Συλλόγων στην Αθήνα, στις 28 Απριλίου. Η ενημέρωση έγινε από δύο μέλη της Αρχής Προστασίας Προσωπικών Δεδομένων, την πρόεδρο της Νομοπαρασκευαστικής επιτροπής για το σχετικό Νομοσχέδιο, την πρόεδρο του Τομέα Ηλεκτρονικών Υγείας του Ινστιτούτου Επιστημονικών Ερευνών του ΠΙΣ και τον πρόεδρο του Ελληνικού Συνδέσμου Πληροφορικής Υγείας (δηλαδή τα πλέον αρμόδια και έγκυρα πρόσωπα). Βασίζονται επίσης σε κατάλογο σχετικών ερωτήσεων – απαντήσεων που δημοσίευσε τις επόμενες μέρες ο Ιατρικός Σύλλογος Θεσσαλονίκης.

Μπορείτε ακόμη να ανατρέξετε στην ανακοίνωση που εξέδωσε ο Ιατρικός Σύλλογος Αθηνών στις 16 Μαΐου: http://www.isathens.gr/syndikal/7825-synoptikes-odigies-symmorfosis-id-iatreiou-gdpr.html όπου περιλαμβάνεται και υπόδειγμα αρχείου επεξεργασίας ευαίσθητων δεδομένων.

Σε κάθε περίπτωση, αυτή η ενημέρωση (όπως και το κείμενο του ΙΣΑ) περιλαμβάνουν απλή πληροφόρηση, δεν αποτελούν οδηγίες, ούτε συνεπάγονται την ανάληψη οποιουδήποτε είδους ευθύνης από το Σύλλογο ή τον πρόεδρο για τυχόν προβλήματα που θα προκύψουν.

Από την άλλη πλευρά, ο GDPR φαίνεται σε πολλές εταιρείες πληροφορικής και νομικής σαν ένα «πεδίο δράσεως λαμπρό», όπου θα «πουλήσουν φύκια για (περιττές) μεταξωτές κορδέλες στα κορόιδα». Ήδη ο Σύλλογος (και φαντάζομαι η αλληλογραφία πολλών από σας) κατακλύζονται από

πλήθος προσφορών και προτάσεων, οι οποίες είναι παραδείγματα ασάφειας και σκόπιμης χρήσης τεχνικής ορολογίας για πρόκληση σύγχυσης και ανασφάλειας. Ας προσέχουμε λοιπόν και από δεξιά και από αριστερά…

- Σκοπός του GDPR είναι η κατάργηση των προληπτικών διαδικασιών (π.χ. αδειοδοτήσεων από τις αρμόδιες αρχές για συγκέντρωση και επεξεργασία δεδομένων) και η μεταφορά της ευθύνης στο χειριστή των πληροφοριών, ο οποίος θα πρέπει να τηρεί κάποιες διαδικασίες και να έχει στο αρχείο του στοιχεία τα οποία θα αποδεικνύουν την τήρηση των διαδικασιών. Ο έλεγχος δηλαδή δεν θα είναι προληπτικός αλλά κατασταλτικός και δειγματοληπτικός.
- Ο GDPR εφαρμόζεται και στα ιδιωτικά ιατρεία με κλιμακούμενες, όμως, υποχρεώσεις ανάλογα με το μέγεθος – κίνηση του κάθε Ιατρείου, την ποσότητα των πληροφοριών που συγκεντρώνονται, το είδος της επεξεργασίας των δεδομένων και την επικινδυνότητα της επεξεργασίας για τα δικαιώματα και τις ελευθερίες των υποκειμένων (αυτών τους οποίους αφορούν οι πληροφορίες).
- Είδη δεδομένων: Τα παραδοσιακά (υγείας, δημογραφικά, ασφαλιστικά κλπ) αλλά και τα νεώτερα (π.χ. βιομετρικά, γενετικά).
- Αρχή του Σκοπού: Τα δεδομένα θα συλλέγονται για ένα συγκεκριμένο και καθορισμένο σκοπό.
- Αρχή της Λογοδοσίας: Ο υπεύθυνος θα πρέπει να αποδείξει ότι τηρεί όλους τους απαραίτητες διαδικασίες.
- Αρχή της Ελαχιστοποίησης: Θα συλλέγονται μόνον τα απολύτως απαραίτητα δεδομένα για τον σκοπό για τον οποίο προορίζονται και όχι περιττά.
- Αρχή των Ψευδωνύμων: Θα χρησιμοποιούνται ψευδώνυμα όπου είναι δυνατόν.
- Αρχή της Κωδικοποίησης: Τα δεδομένα θα κωδικοποιούνται κι θα προστατεύονται με επαρκείς κωδικούς εισόδου.
- Αρχή του Σχεδιασμού: Η ιδιωτικότητα και η προστασία των προσωπικών δεδομένων θα λαμβάνονται υπ’ όψη εξ αρχή,ς κατά το σχεδιασμό των συστημάτων. Οι προεπιλεγμένες ρυθμίσεις θα είναι οι προσφορότερες για την ασφάλεια και την ιδιωτικότητα.
- Απαγορεύεται η επεξεργασία των δεδομένων εκτός εξαιρέσεων (π.χ. Προστασία δημόσιας υγείας, προληπτική – επαγγελματική Ιατρική, Εκτίμηση ικανότητας προς εργασία – οδήγηση – χειρισμό μηχανημάτων, Εφαρμογή κοινωνικών μέτρων, Διαχείριση συστημάτων υγείας)
- Η επεξεργασία γίνεται μόνο μετά από ρητή και έγγραφη συγκατάθεση του υποκειμένου.
- Πρέπει να τηρείται Αρχείο Δραστηριοτήτων Επεξεργασίας.
- Σε περίπτωση παραβίασης θα ενημερώνεται η Αρχή Προστασίας Προσωπικών Δεδομένων μέσα σε 72 ώρες και θα γίνεται εκτίμηση των επιπτώσεων της παραβίασης για τα υποκείμενα. Αν οι επιπτώσεις της παραβίασης εκτιμηθούν ως κρίσιμες για τα υποκείμενα, θα ενημερώνονται και οι ίδιοι.

- Τα ατομικά και τα μικρά Ιατρεία και Εργαστήρια δεν έχουν υποχρέωση ορισμού Υπευθύνου Προστασίας Δεδομένων.
- Δημόσιες αρχές όμως (π.χ. οι Ιατρικοί Σύλλογοι) και μεγάλης κλίμακας οργανισμοί (π.χ. Κλινικές, Νοσοκομεία) έχουν την παραπάνω υποχρέωση.
- Τεκμηρίωση: Ποιος; (ποιος είναι ο υπεύθυνος για την συγκέντρωση, την επεξεργασία και την ασφάλεια των δεδομένων). Γιατί; (σκοπός συγκέντρωσης & επεξεργασίας). Τι; (Τι είδους δεδομένα συλλέγονται και από ποια υποκείμενα). Που; (Σε ποιόν στέλνονται). Εκτός ΕΕ; (Εάν διαβιβάζονται σε χώρες εκτός της Ευρωπαϊκής Ένωσης). Πόσο; (Για πόσο χρονικό διάστημα θα διατηρηθούν). Πώς; (Γενική περιγραφή μέτρων ασφαλείας). *Σχετικά δείτε και το «υπόδειγμα αρχείου επεξεργασίας ευαίσθητων δεδομένων» του ΙΣΑ που προανέφερα*.
- Η προσέλευση του ασθενούς στο Ιατρό δηλώνει - σαν πράξη από μόνη της - ότι ήδη υπάρχει σχέση αμοιβαίας εμπιστοσύνης και συγκατάθεσης εκ μέρους του ασθενή για χρήση των προσωπικών του δεδομένων για τους σκοπούς της διάγνωσης και της θεραπείας (αποκλειστικά).
- Ο Ιατρός έχει υποχρέωση να τηρεί (ψηφιακό ή όχι) αρχείο των ασθενών του. Το αρχείο πρέπει να περιλαμβάνει ονοματεπώνυμο, πατρώνυμο, ηλικία, φύλο, επάγγελμα, διεύθυνση, ημερομηνίες επισκέψεων, και κάθε άλλο ουσιώδες στοιχείο που συνδέεται με την παροχή φροντίδας στον ασθενή, όπως τα ενοχλήματα της υγείας του και το λόγο της επίσκεψης, την πρωτογενή και δευτερογενή διάγνωση ή την αγωγή που ακολουθήθηκε.
- Ο GDPR εφαρμόζεται και στην περίπτωση που τα αρχεία δεν είναι ηλεκτρονικά αλλά χειρόγραφα.
- Η Εφορία έχει το δικαίωμα να ελέγξει το Ιατρικό αρχείο (παρά το γεγονός ότι αυτό περιλαμβάνει ευαίσθητα προσωπικά δεδομένα των ασθενών).
- Εάν ο ασθενής ζητήσει αντίγραφα των δεδομένων που τον αφορούν, είμαστε υποχρεωμένοι να τα δώσουμε.
- Επίσης πρέπει να προβούμε στις αναγκαίες διορθώσεις ή συμπληρώσεις δεδομένων προσωπικού χαρακτήρα του ασθενή, αν μας το ζητήσει ο ίδιος.
- Ο ασθενής τέλος, μπορεί να ζητήσει να διαγράψουμε στοιχεία προσωπικού χαρακτήρα για τον ίδιο και πρέπει να το κάνουμε, εκτός εάν υπάρχει νόμιμος λόγος να τα διατηρήσουμε.
- Τα στοιχεία διατηρούνται για 10 χρόνια από την τελευταία επίσκεψη.
- Γνωματεύσεις υγείας και ικανότητας οδήγησης, αθλητισμού, χειρισμού μηχανημάτων, όπλων κλπ συνεχίζουν να εκδίδονται κανονικά λαμβάνοντας πρόνοια να μη περιλαμβάνουν παραπάνω από τα απολύτως απαραίτητα στοιχεία.
- Το ίδιο ισχύει και για τις γνωματεύσεις ασθένειας και απουσίας από το σχολείο ή την εργασία.
- Το ποσό τού προστίμου (μέχρι 20 εκατομμύρια €!) που ορίζει ο GDPR είναι το ανώτατο. Εξαρτάται από τον κύκλο εργασιών της εταιρείας, τη φύση και τη βαρύτητα της παράβασης κ. ά.

- Χρήση ηλεκτρονικού ταχυδρομείου για ανταλλαγή πληροφοριών σχετικών με ασθενείς μεταξύ Ιατρών (π.χ. μεταξύ εργαστηριακού και κλινικού) γίνεται εφ' όσον λαμβάνονται τα κατάλληλα μέτρα ασφαλείας. Οι περισσότερες εταιρείες ηλεκτρονικού ταχυδρομείου (π.χ. otenet.gr) ήδη κωδικοποιούν τα μηνύματα.
- Τα μέσα κοινωνικής δικτύωσης χρησιμοποιούνται μόνον για ανωνυμοποιημένες πληροφορίες, δηλαδή αν ο ασθενής δεν μπορεί να ταυτοποιηθεί από αυτές.
- Επικοινωνία με τον ασθενή μέσω ηλεκτρονικού ταχυδρομείου μπορεί να γίνει μόνον αν ο ίδιος έχει συγκατατεθεί εγγράφως δίνοντας ταυτόχρονα την ηλεκτρονική του διεύθυνση.
- Όλα τα παραπάνω αφορούν κυρίως (από οργανωτική άποψη) τους ελεύθερους επαγγελματίες, αλλά και οι δημόσιοι ή ιδιωτικοί υπάλληλοι Ιατροί, έχουν - όπως εξυπακούεται - ευθύνη για τα προσωπικά δεδομένα ασθενών τα οποία χειρίζονται οι ίδιοι ή περιέρχονται στην αντίληψή τους στα πλαίσια της άσκησης των καθηκόντων τους.

Ο Πρόεδρος

Δρ Άγγελος Βάκαλος
Ωτορινολαρυγγολόγος