Ο εργοθεραπευτής οφείλει να προβεί κατά ελάχιστο στις παρακάτω ενέργειες:

1. **Κατανόηση νομικής βάσης επεξεργασίας προσωπικών δεδομένων**
   - Ο εργοθεραπευτής κατά την άσκηση των καθηκόντων του, επεξεργάζεται δεδομένα προσωπικού χαρακτήρα και μάλιστα πρόκειται για «επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα» (Αρ. 9 ΓΚΠΔ) (*ευαίσθητα προσωπικά δεδομένα* κατά προγενέστερο ορισμό). Επειδή λοιπόν η επεξεργασία είναι απαραίτητη για λόγους «.. *προληπτικής ιατρικής* …. » και «*…παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών*….», σύμφωνα με το άρθρο9 παρ.2 , είναι σαφές ότι **ΔΕΝ απαιτείται συγκατάθεση** από το «υποκείμενο» επεξεργασίας (ασθενή). Φυσικά, εφόσον τα δεδομένα αυτά χρησιμοποιηθούν **ΜΟΝΟ για** το **σκοπό** για τον οποίο προορίζονται και όχι πέραν αυτού.
   - Σε περιπτώσεις κατά τις οποίες τα προσωπικά δεδομένα χρησιμοποιηθούν για άλλο σκοπό είτε πρόκειται να διαβιβαστούν σε τρίτους , θα πρέπει να υπάρχει συγκατάθεση του «υποκείμενου» (π.χ. του ασθενούς)
2. **Να τηρεί (<u>υποχρεωτικά</u>) τα παρακάτω αρχεία (ηλεκτρονικά και σε φυσικό αρχείο)**
   - Αρχείο δραστηριοτήτων υπευθύνου επεξεργασίας [*αρ. 30 ΓΚΠΔ (ΕΕ) 679/2016*]
   - Αρχείο δραστηριοτήτων εκτελούντων επεξεργασίας [*αρ. 30 ΓΚΠΔ (ΕΕ) 679/2016*]
3. Να **συνάπτει** (**υποχρεωτικά**) «δήλωσης εμπιστευτικότητας», μεταξύ επιχείρησης και εργαζομένου, εφόσον ο εργαζόμενος έχει πρόσβαση σε προσωπικά δεδομένα ασθενούς (φυσικό ή ηλεκτρονικό αρχείο) και άρα καθίσταται «εκτελών την επεξεργασία» (π.χ. γραμματέας η οποία έχει πρόσβαση σε καρτέλες ή βιβλία ασθενούς) [*αρ. 28 ΓΚΠΔ (ΕΕ) 679/2016*]
4. Να **συνάπτει** (**υποχρεωτικά**) «δήλωσης εμπιστευτικότητας», μεταξύ επιχείρησης και οποιουδήποτε εξωτερικού συνεργάτη διαβιβάζονται δεδομένα προσωπικού χαρακτήρα ασθενούς (π.χ. Ιατρός, διαγνωστικό εργαστήριο) [*αρ. 28 ΓΚΠΔ (ΕΕ) 679/2016*]
5. Να έχει **κατανοήσει πλήρως, να σέβεται και να διευκολύνει την άσκηση των δικαιωμάτων ενημέρωσης**, πρόσβασης, διόρθωσης και διαγραφής του «υποκείμενου επεξεργασίας» [Αρ. 12-20 ΓΚΠΔ]. Συγκεκριμένα :
   - Σε περίπτωση κατά την οποία το «υποκείμενο» (π.χ. ασθενής), αιτηθεί ενημέρωση για το ποια στοιχεία επεξεργάζεται ο «υπεύθυνος επεξεργασίας» (εργοθεραπευτής), θα πρέπει :
     - Εντός χρονικού **διαστήματος ενός (1) μηνός**, ο «υπεύθυνος επεξεργασίας» να απαντήσει γραπτώς. Σε περίπτωση που έχει ζητηθεί, θα πρέπει να αναφέρονται λεπτομερώς και με διαφάνεια οι λόγοι επεξεργασίας, η νομική βάση, οι αποδέκτες, το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (ΑΠΔΠΧ)
6. **Να εφαρμόσει κατάλληλα οργανωτικά και τεχνικά μέτρα** με σκοπό την ασφάλεια δεδομένων και την ασφάλεια της επεξεργασίας [*Αρ. 24 ΓΚΠΔ*].
   - Η ενέργεια αυτή, διαφοροποιείται ανάλογα με τις διαδικασίες που εφαρμόζει η κάθε επιχείρηση (π.χ. εργαστήριο εργοθεραπείας) κα τα συστήματα πληροφορικής (λογισμικό & υλικό) που χρησιμοποίει. Συνεπώς, λόγω του ότι είναι σχεδόν αδύνατον να καλύψουμε εντός του παρόντος κειμένου όλες τις πιθανές περιπτώσεις, παρόλα αυτά σας

παραθέτουμε κάποια «κοινά παραδείγματα» καλής πρακτικής εφαρμογής μέτρων ασφαλείας και προστασίας των δεδομένων.

- Το φυσικό αρχείο (π.χ. παραπεμπτικά, καρτέλες- φάκελοι ασθενούς), θα πρέπει να φυλάσσεται σε χώρο (π.χ. ερμάριο) ο οποίος να μην είναι προσβάσιμος από μη εξουσιοδοτημένα άτομα
- Δεν θα πρέπει να υπάρχει οποιασδήποτε μορφής αρχείο (π.χ. μια αίτηση), έστω και προσωρινά προσβάσιμο και ορατό από τρίτους
- Ο υπολογιστής που χρησιμοποιούμε, θα πρέπει υποχρεωτικά να επιτρέπει είσοδο μόνο με κωδικό πρόσβασης. Επιθυμητή ενέργεια επίσης, είμαι η διαβαθμισμένη πρόσβαση σε υπολογιστή με διαφορετικά δικαιώματα για κάθε χρήστη.
- Εάν πιθανώς χρησιμοποιούμε αρχεία, Excel, Word, Αρχεία κειμένου, με δεδομένα προσωπικού χαρακτήρα, προτείνουμε τα αρχεία αυτά να προστατεύονται με κωδικό πρόσβασης.
- Όταν ανταλλάσσονται μηνύματα ηλεκτρονικού ταχυδρομείου (email) (π.χ. αποστολή ή λήψη κάποιων δεδομένων από/προς συνεργαζόμενο Ιατρό), συστήνουμε τα αρχεία αυτά να προστατεύονται με κωδικό πρόσβασης.
- Πλήρης καταγραφή συστήματος πληροφορικής (εάν υπάρχει). Θα πρέπει να έχουμε σαφή εικόνα για το πληροφοριακό σύστημα που χρησιμοποιούμε και συγκεκριμένα να απαντήσουμε άμεσα στα εξής κρίσιμα ερωτήματα :
    1. Που αποθηκεύονται τα δεδομένα
    2. Υπάρχει βάση δεδομένων; Είναι κρυπτογραφημένη ; Αν ναι, ποια δεδομένα είναι και ποια όχι;
    3. Ποιοί έχουν πρόσβαση σε αυτό το σύστημα και με ποιά δικαιώματα; Τι ενέργειες πραγματοποιούν οι χρήστες ; Υπάρχει διαβάθμιση;
    4. Υπάρχουν αντίγραφα ασφαλείας ; Αν ναι που βρίσκονται; Κάθε πότε δημιουργούνται ; ποιος και με ποιόν τρόπο έχει πρόσβαση σε αυτά; Υπάρχει σχέδιο ανάκαμψης ;
- Έλεγχος συμμόρφωσης (π.χ. εταιρικό WebSite εργαστηρίου εργοθεραπείας)
    1. Θα πρέπει να γίνουν οι ως άνω έλεγχοι (δλδ. Ως πληροφοριακό σύστημα) και επιπλέον:
        - Να ελεγχθούν και να αναθεωρηθούν εάν κριθεί απαραίτητο οι όροι χρήσης του και να δοθεί ιδιαίτερο βάρος στην πολιτική που λαμβάνει ο επισκέπτης (σημ: για να λάβει ο επισκέπτης Cookie analytics μέσω ιστοσελίδας, θα πρέπει υποχρεωτικά να έχει αποδεχθεί αυτό τον όρο)
        - Σε οποιαδήποτε φόρμα επικοινωνίας εντός WebSite, θα πρέπει υποχρεωτικά να υπάρχει η δυνατότητα «συναίνεσης» του επισκέπτη, χωρίς την οποία δεν θα πρέπει να αποστέλλονται τα στοιχεία μέσω φόρμας

7. **Να γνωρίζει τις ενέργειες που πρέπει να πράξει**, σε περίπτωση παραβίασης και πως ενεργούμε κατά την «Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή» [Αρ.33 ΓΚΠΔ]

- Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός **72 ωρών** από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή (ΑΠΔΠΧ)
- Η γνωστοποίηση πραγματοποιείται με την αποστολή συγκεκριμένου εγγράφου και αποστέλλετε σε προκαθορισμένη ηλεκτρονική διεύθυνση

8. **Να κατανοήσει πλήρως την «αρχή της λογοδοσίας»** [Αρ. 5 παρ 2]
   - Σύμφωνα με την «αρχή της λογοδοσίας», ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση («λογοδοσία»).
   - Ως εκ τούτου δεν είναι αρκετό το απλά να αναγνώσει κανείς τον ΓΚΠΔ είτε να διαδίδει τη συμμόρφωσή του, αλλά θα πρέπει να είναι σε θέση ανά πάσα στιγμή και όποτε χρειαστεί, να «αποδεικνύει» την συμμόρφωση του
   - Ως καλή πρακτική συμμόρφωσης με την αρχή της λογοδοσίας, θα πρέπει, όλα τα έγγραφα (υποχρεωτικά και μη) τα οποία χρησιμοποιείται και αναλύθηκαν στις ανωτέρω παραγράφους, να φυλάσσονται σε φυσικό φάκελο. (π.χ. φάκελος αρχείου ΓΚΠΔ-, ή φάκελος Ενεργειών ΓΚΠΔ)

- Οι παραπάνω οδηγίες συμμόρφωσης, αποτελούν συνοπτικό οδηγό και αφορούν στις κατά ελάχιστον υποχρεώσεις ενός εργοθεραπευτή ή εργαστηρίου εργοθεραπείας.
- Πιθανώς οι ενέργειες αυτές να διαφοροποιούνται ανάλογα με το προσωπικό που απασχολείται (π.χ. σε κάποιο εργαστήριο), είτε ειδικών διαδικασιών, συστημάτων πληροφορικής που πιθανώς κάποιος επαγγελματίας να εφαρμόζει και να χρησιμοποιεί κατά περίπτωση και να μην έχει προβλεφθεί μέσω του παρόντος κειμένου.

Για οποιαδήποτε απορία που αφορά αποκλειστικά σε θέματα προστασίας δεδομένων προσωπικού χαρακτήρα, παρακαλούμε να στείλετε email στην διεύθυνση: privacy@pse.org.gr

Τα ερωτήματα θα συγκεντρωθούν, έτσι ώστε να απαντηθούν αρχικά με τη μορφή ερωτήσεων – απαντήσεων.