



Κώδικας Δεοντολογίας και Εμπιστευτικότητας Γενικού Νοσοκομείου Αγρινίου

1. Εισαγωγή

Η προστασία των προσωπικών δεδομένων των φυσικών και ιδιαιτέρως η διαχείριση των ευαίσθητων προσωπικών δεδομένων ασθενών και εργαζομένων αποτελεί πρωταρχικό μέλημα της διοίκησης του ΓΝΑ. Στα πλαίσια της συμμόρφωσης με τη νέα νομοθεσία (ΕΕ 2016/679) υιοθετείται ο παρών Κώδικας Δεοντολογίας & Εμπιστευτικότητας για την Προστασία των Δικαιωμάτων του Ατόμου κατά την επεξεργασία των προσωπικών του δεδομένων εντός και εκτός του Νοσοκομείου. Ο συγκεκριμένος Κώδικας αποτελεί διακήρυξη των Αρχών και των Αξιών του ΓΝΑ όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

2. Αρχές

Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ιδίως ευαίσθητων δεδομένων υγείας, θα πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο. Κατά συνέπεια, η διοίκηση και οι εργαζόμενοι του Νοσοκομείου ενστερνίζονται και εφαρμόζουν τις παρακάτω αρχές κατά την τέλεση των καθηκόντων τους:

1. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα· πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την **αρχή της επικουρικότητας & αναλογικότητας**.
2. Η **αρχή της διαφάνειας** απαιτεί οποιαδήποτε ενημέρωση που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και εύκολα κατανοητή και να χρησιμοποιείται σαφής και απλή διατύπωση και επιπλέον, κατά περίπτωση, απεικόνιση.
3. Η **αρχή της προσβασιμότητας** εξασφαλίζει το δικαίωμα του παρόχου των δεδομένων στην πρόσβαση και στην διόρθωση αυτών.
4. Η **αρχή της λογοδοσίας** υποχρεώνει τη διοίκηση να γνωστοποιήσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, εκτός εάν ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει, ότι η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.
5. Η **Αρχή της ελαχιστοποίησης** των δεδομένων υποχρεώνει το Νοσοκομείο να συλλέγει και να κατακρατά μόνο τα δεδομένα που είναι τελείως απαραίτητα για την εξυπηρέτηση των εννόμων συμφερόντων αυτής και να τα διαγράφει με το πέρας αυτών.

3. Προστασία Προσωπικών Δεδομένων

Προκειμένου να αποφευχθεί οποιαδήποτε διαρροή προσωπικών δεδομένων ή κάποια άλλη παραβατική συμπεριφορά ως προς τη νέα νομοθεσία, η διοίκηση και το προσωπικό δεσμεύονται ότι:

1. Δεν επιτρέπεται η οποιαδήποτε συλλογή προσωπικών δεδομένων που δεν είναι αυστηρά απαραίτητη για τους νόμιμους εργασιακούς ή/και θεραπευτικούς σκοπούς του ΓΝΑ.
2. Κατά την συλλογή ευαίσθητων δεδομένων (δεδομένα υγείας, ποινικά κ.α.), συλλέγεται υποχρεωτικά η συγκατάθεση τού ασθενούς ή των λοιπών υποκειμένων των δεδομένων.
3. Η συγκατάθεση του υποκειμένου παρακάμπτεται κατ' εξαίρεση μόνο όταν η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, ή όταν ο κηδεμόνας παιδιού είναι σωματικά ή νομικά ανίκανος να συγκατατεθεί.
4. Τα ευαίσθητα προσωπικά δεδομένα πρέπει σε κάθε περίπτωση να μην βρίσκονται εκτεθειμένα ανεξέλεγκτα στο χώρο του Νοσοκομείου και αποθηκεύονται με ασφαλή τρόπο.
5. Η ευθύνη προστασίας των προσωπικών δεδομένων και η τήρηση των παραπάνω κατανέμεται αρχικά στη διοίκηση και στη συνέχεια σε όλους τους εργαζομένους που έχουν πρόσβαση σε αυτά.

4. Κανόνες Διαδικτυακής Συμπεριφοράς

1. Για την δημοσιοποίηση δεδομένων εικόνας απαραίτητη είναι η συλλογή της συγκατάθεσης του ασθενούς.
2. Οι φωτογραφίες δε θα πρέπει σε καμία περίπτωση να συνοδεύονται από λεζάντες οι οποίες να αφορούν προσωπικές πληροφορίες για τους νοσηλευόμενους όπως το όνομα ή την στοιχεία επικοινωνίας τους.
3. Μη δημοσιοποίηση αποτελεσμάτων ερευνών που θίγουν την κοινωνική προέλευση των ασθενών ή την οικογενειακή τους κατάσταση.
4. Μη χρησιμοποίηση υβριστικής γλώσσας και αποφυγή χρήσης εννοιών ή λέξεων που προσβάλλουν.
5. Χρήση μόνο πληροφοριών των οποίων μπορεί να εξακριβωθεί η εγκυρότητά τους (στοιχεία του συγγραφέα, της βιβλιογραφίας, της προέλευσης της ιστοσελίδας κτλ.).
6. Μη τοποθέτηση συνδέσμων (LINKS) σε υπηρεσίες όπως δωμάτια συνομιλίας, ιστολόγια (blogs και προσωπικές ιστοσελίδες των οποίων η εγκυρότητα δεν μπορεί να εξακριβωθεί).

5. Πρόσθετα Τεχνικά Μέτρα Ασφαλείας

Πέραν των προαναφερθέντων, η διοίκηση και το προσωπικό του ΓΝΑ οφείλουν να λαμβάνουν τις απαραίτητες προφυλάξεις σε τεχνικό επίπεδο και να φροντίζουν τα παρακάτω:

1. Χρήση ισχυρών/δύσκολων κωδικών για την είσοδο στα συστήματα και στις εφαρμογές και τακτικές αλλαγές τους.
2. Χρήση μοντέρνων λειτουργικών συστημάτων υπολογιστή και διαρκής ενημέρωσή τους.
3. Αποφυγή χρήσης λογισμικού ελεύθερης χρήσης (free download).
4. Κρυπτογράφηση τοπικού δίσκου υπολογιστή μέσω του λειτουργικού συστήματος.
5. Κρυπτογράφηση εξωτερικών μονάδων αποθήκευσης (πχ εξωτερικός σκληρός δίσκος, USB κ.ο.κ.) .
6. Αποφυγή χρήσης και παραχώρησης προνομιακών δικαιωμάτων πρόσβασης στον απλό χρήστη (δικαιώματα Local Administrator) .
7. Αποφυγή χρήσης ελεύθερων email, πχ Yahoo, για αποστολή και λήψη ευαίσθητων δεδομένων, πχ ιατρικών εξετάσεων.

6. Κανόνες Εμπιστευτικότητας Δεδομένων

Το Γενικό Νοσοκομείο Αγρινίου, στα πλαίσια της άσκησης της δραστηριότητάς του και για τους σκοπούς αυτούς, συλλέγει και επεξεργάζεται δεδομένα φυσικών προσώπων (ασθενών πελατών, προμηθευτών, εξωτερικών συνεργατών, εργαζομένων), φέρει την ιδιότητα του

Υπευθύνου Επεξεργασίας Προσωπικών Δεδομένων σύμφωνα με τη νομοθεσία (Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ., καθώς τηρεί αρχεία και προβαίνει σε επεξεργασία δεδομένων προσωπικού χαρακτήρα (προσωπικών δεδομένων), καθορίζοντας το σκοπό και ορίζοντας τα μέσα της επεξεργασίας αυτών.

Στο πλαίσιο αυτό, η διοίκηση και οι εργαζόμενοι συμφωνούν, συνομολογούν, αποδέχονται και δεσμεύονται ως προς τα εξής:

1. Ο εργαζόμενος φέρει την υποχρέωση να αντιμετωπίζει ως εμπιστευτικές τις πληροφορίες που αφορούν φυσικά πρόσωπα (ασθενείς, πελάτες, συνεργάτες, προμηθευτές, άλλοι εργαζόμενοι, τις οποίες γνωρίζει ή/και στις οποίες αποκτά πρόσβαση στο πλαίσιο της εκπλήρωσης της εργασίας που έχει αναλάβει / της άσκησης των καθηκόντων του που του έχουν ανατεθεί ή και επ' ευκαιρία αυτής/ αυτών.
2. Ο εργαζόμενος αναλαμβάνει την υποχρέωση να προστατεύει και να διαφυλάττει τον απόρρητο χαρακτήρα των προσωπικών δεδομένων που τηρεί και επεξεργάζεται το ΓΝΑ, σύμφωνα με τις εντολές και οδηγίες του.
3. Ο εργαζόμενος αναλαμβάνει την υποχρέωση να χρησιμοποιεί ή εν γένει να επεξεργάζεται τα προσωπικά δεδομένα σύμφωνα με τις εντολές και υποδείξεις της διοίκησης και μόνο για τον σκοπό για τον οποίο γίνεται η εκάστοτε επεξεργασία.
4. Ο εργαζόμενος υποχρεούται να συμμορφώνεται και να ακολουθεί τις εντολές, υποδείξεις και οδηγίες που έχει λάβει ειδικά από τον διοίκηση ή γνωρίζει λόγω της φύσης της εργασίας ή των καθηκόντων του αναφορικά με τα μέτρα φυσικής, οργανωτικής και τεχνικής ασφάλειας για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των προσωπικών δεδομένων.

Ο ΔΙΟΙΚΗΤΗΣ
ΜΙΧΑΗΛ ΣΕΡΑΣΚΕΡΗΣ