ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Eurobank

Secure HealthData

ΑΣΦΑΛΕΙΑ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΥΓΕΙΑ

"Προστασία ευαίσθητων προσωπικών δεδομένων από τη θεωρία στην πράξη. Βέλτιστες πρακτικές κατά τη χρήση ηλεκτρονικού υπολογιστή στους χώρους εργασίας"

Τσιπούρης Ελευθέριος

Υπάλληλος Πληροφορικής, Τμήμα Πληροφορικής – Γενικό Νοσοκομείο Ξάνθης

ΠΡΟΣΤΑΣΙΑ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΤΗ ΘΕΩΡΙΑ ΣΤΗΝ ΠΡΑΞΗ. ΒΕΛΤΙΣΤΕΣ ΠΡΑΚΤΙΚΕΣ ΚΑΤΑ ΤΗ ΧΡΗΣΗ Η/Υ ΣΤΟΥΣ ΧΩΡΟΥΣ ΕΡΓΑΣΙΑΣ

ΤΣΙΠΟΥΡΗΣ ΕΛΕΥΘΕΡΙΟΣ
ΗΛΕΚΤΡΟΛΟΓΟΣ ΜΗΧΑΝΙΚΟΣ ΚΑΙ ΜΗΧΑΝΙΚΟΣ ΥΠΟΛΟΓΙΣΤΩΝ
ΥΠΑΛΛΗΛΟΣ ΤΟΥ ΤΜΗΜΑΤΟΣ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΟΥ ΓΕΝΙΚΟΥ ΝΟΣΟΚΟΜΕΙΟΥ ΞΑΝΘΗΣ

ΓΕΝΙΚΑ ΓΙΑ ΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ο καινούργιος κανονισμός που έχει άμεση εφαρμογή ενιαία σε όλη την Ε.Ε. από τις 25 Μαΐου 2018 και δεν χρειάζεται τα κράτη μέλη να ενσωματώσουν τις διατάξεις του στην εθνική νομοθεσία τους, αυξάνει σημαντικά το επίπεδο προστασίας των προσωπικών δεδομένων των πολιτών. Αυξάνει ταυτόχρονα όμως και τις υποχρεώσεις τους και το βαθμό υπευθυνότητας που πρέπει να δείχνουν και οι ίδιοι, ιδίως στο κομμάτι της ταυτοποίησής τους και της έγκαιρης ενημέρωσης της Δημόσιας Διοίκησης. Το ίδιο συμβαίνει και από την πλευρά της Δημόσιας Διοίκησης και τους υπαλλήλους που εμπλέκονται στην επεξεργασία των δεδομένων αυτών, προσθέτοντας δυστυχώς δουλειά και γραφειοκρατία. Σημαντικός θα είναι ο συμβουλευτικός ρόλος του Υ.Π.Δ. που θα πρέπει να γνωμοδοτεί για τις διάφορες περιπτώσεις που θα προκύψουν στην πράξη, είτε ο ίδιος, είτε συμβουλευόμενος την Α.Π.Π.Δ. Ενδέχεται να υπάρξουν κάποιες αλλαγές όταν ψηφιστεί ο σχετικός νόμος που είναι εδώ και κάποιους μήνες προς ψήφιση στη Βουλή, κάτι που προτείνεται να γίνει από τον κανονισμό. Με το νέο νόμο θα καταργηθεί ο ισχύον Νόμος 2472/1997 και θα τεθούν σε ισχύ διατάξεις που συμπληρώνουν τον Κανονισμό και εξειδικεύουν ορισμένες από τις υποχρεώσεις που θεσπίζει ο Κανονισμός.

- Μεγάλα τα πρόστιμα για τις παραβάσεις.

- Μεγάλη περιπτωσιολογία και πρακτική δυσκολία στην εφαρμογή του.

ΠΟΙΑ ΕΙΝΑΙ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ;

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως:

1.Στοιχεία αναγνώρισης με τα κυριότερα να είναι:

Α.Ονοματεπώνυμο

Β.Ηλικία

Γ.Κατοικία

Δ.Επάγγελμα

Ε.Οικογενειακή κατάσταση

2. Φυσικά χαρακτηριστικά
3. Εκπαίδευση
4. Εργασία (Προϋπηρεσία, εργασιακή συμπεριφορά κλπ.)
5. Οικονομική κατάσταση
6. Ενδιαφέροντα
7. Δραστηριότητες
8. Συνήθειες

ΠΟΙΑ ΕΙΝΑΙ ΤΑ ΕΥΑΙΣΘΗΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ;

1. Φυλετική ή εθνική προέλευση
2. Πολιτικά φρονήματα
3. Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
4. Συμμετοχή σε συνδικαλιστική οργάνωση
5. Ερωτική ζωή
6. Ποινικές διώξεις και καταδίκες
7. Κοινωνική πρόνοια
8. Υγεία

ΕΥΑΙΣΘΗΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΗΝ ΥΓΕΙΑ

1. Το νοσηλευτικό ίδρυμα υποχρεούται με βάση το νόμο 3418/2005(αρθ. 14, παρ. 4) να τηρεί τα ιατρικά αρχεία για μια εικοσαετία από την τελευταία επίσκεψη του ασθενούς. Δεκαετία στους ιδιώτες ιατρούς
2. Οι φάκελοι που περιέχουν προσωπικά δεδομένα (φυσικό αρχείο) πρέπει να είναι τοποθετημένοι σε φωριαμούς (επιθυμητό να κλειδώνουν) και να μην εκτίθενται σε κοινή θέα. - Αφορά ενδεικτικά τις γραμματείες των κλινικών, τις διοικητικές υπηρεσίες, τον εργαστηριακό τομέα και τα ΤΕΠ.
3. Δεν θα πρέπει να αφήνονται εκτεθειμένα, χωρίς επίβλεψη, έγγραφα και φορητά μέσα αποθήκευσης πάνω σε γραφεία. -Αφορά τους πάντες.
4. Όταν σε ένα γραφείο εκτίθενται προσωπικά δεδομένα και πρέπει ο τελευταίος υπάλληλος του γραφείου αυτού να εξέλθει, θα πρέπει να κλειδώνει τη πόρτα κάθε φορά.

ΕΥΑΙΣΘΗΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΗΝ ΥΓΕΙΑ

5. Όσον αφορά τα προσωπικά δεδομένα των εργαζομένων στο δημόσιο, η συλλογή τους και η επεξεργασία τους προβλέπεται με ακρίβεια στο άρθρο 23 του δημοσιοϋπαλληλικού κώδικα.

Στην περίπτωση της επεξεργασίας των προσωπικών δεδομένων των ασθενών το Άρθρο 9, παρ. 2, περίπτωση (η) του Γ.Κ.Π.Δ. επιτρέπει την επεξεργασία των προσωπικών δεδομένων όταν είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3, όπου εκεί αναφέρεται ότι τα ευαίσθητα δεδομένα προσωπικού χαρακτήρα μπορεί να τύχουν επεξεργασίας για τους σκοπούς που προβλέπονται στην παράγραφο 2 στοιχείο η), όταν τα δεδομένα αυτά υποβάλλονται σε επεξεργασία από ή υπό την ευθύνη επαγγελματία που υπόκειται στην υποχρέωση τήρησης του επαγγελματικού απορρήτου βάσει του δικαίου της Ένωσης ή κράτους μέλους ή βάσει κανόνων που θεσπίζονται από αρμόδιους εθνικούς φορείς ή από άλλο πρόσωπο το οποίο υπέχει επίσης υποχρέωση τήρησης του απορρήτου βάσει του δικαίου της Ένωσης ή κράτους μέλους ή βάσει κανόνων που θεσπίζονται από αρμόδιους εθνικούς φορείς.

ΕΥΑΙΣΘΗΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΗΝ ΥΓΕΙΑ

6. Όταν οι ασθενείς είναι παιδιά, πρέπει να γίνεται η μέγιστη δυνατή προσπάθεια, με τον προσφορότερο δυνατό τρόπο, για την ταυτοποίηση της ηλικίας τους αλλά και του κηδεμόνα αν είναι μικρότερα από 13 ετών. (Στο σχέδιο Νόμου 15 χρόνια) Η ταυτοποίηση των παραπάνω συνίσταται να γίνεται με το βιβλιάριο υγείας του παιδιού.
7. Οτιδήποτε δίνεται από οποιοδήποτε τμήμα που αφορά τον ασθενή θα πρέπει να δίνεται είτε στον ίδιο, είτε σε εξουσιοδοτημένο πρόσωπο, είτε σε πρόσωπο που έχει υποδείξει ο ίδιος ενυπόγραφα κατά την παραμονή του στο ίδρυμα, είτε στον ιατρό που έδωσε την εντολή για εξετάσεις, είτε σε βοηθό αυτού με την έννοια του αρθ. 13 παρ.$2^{α}$ του Κ.Ι.Δ (Ν3418/2005). Εδώ θα πρέπει να αναφερθεί ότι υπάρχει έντονη περιπτωσιολογία, επίσης και δυσκολία στην πρακτική εφαρμογή.

ΕΥΑΙΣΘΗΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΗΝ ΥΓΕΙΑ

8. Στα ΤΕΠ και στις αίθουσες νοσηλείας των κλινικών θα πρέπει τα αρχεία να μην είναι σε κοινή θέα, και οι γιατροί να ομιλούν όσο χαμηλόφωνα γίνεται, προσφωνώντας ή αναφερόμενοι στον ασθενή με το μικρό του όνομα, και στα κρεβάτια, όπου αναφέρεται, το Ονοματεπώνυμο του ασθενούς να είναι ψευδωνυμοποιημένο. Παρόλα αυτά δεν μπορεί να γίνει πλήρης εφαρμογή και απαιτούνται οδηγίες από την Αρχή Προστασίας Προσωπικών Δεδομένων μέσω του Υπευθύνου Προστασίας Δεδομένων που θα ορίσει με βάση τον Κανονισμό το Νοσοκομείο, είτε εσωτερικά είτε ως εξωτερικό συνεργάτη.
9. Οι αναφορές σε προσωπικά δεδομένα ασθενών έξω από ιατρεία ή εργαζομένων σε πίνακες ανακοινώσεων πρέπει να υπόκεινται σε ψευδωνυμοποίηση, εκτός και αν Νόμος προβλέπει τη δημοσιοποίησή τους.

ΕΥΑΙΣΘΗΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΗΝ ΥΓΕΙΑ

10. Όταν γίνονται συμβάσεις με εξωτερικούς συνεργάτες ή εταιρίες και αυτές έχουν πρόσβαση σε προσωπικά δεδομένα, πρέπει να υπάρχει άρθρο της σύμβασης με ρητή αναφορά στις υποχρεώσεις τους όσον αφορά την προστασία των προσωπικών δεδομένων. Εννοείται ότι αφορά και το συνεργείο καθαριότητας, αλλά και τις εταιρίες πληροφορικής ή με ιδιώτες με τους οποίους έχουμε συμβάσεις για το software και hardware του Νοσοκομείου.

11. Στο Νόμο 3861/2010, την περίφημη Διαύγεια, αναφέρεται αναλυτικά τι είναι υποχρεωμένη να δημοσιοποιεί η Δημόσια Διοίκηση στο άρθρο 2. Όμως στο Άρθρο 5 με τίτλο: Προστασία δεδομένων προσωπικού χαρακτήρα και απόρρητα, αναφέρονται τα εξής: Η ανάρτηση των πράξεων που αναφέρονται στο άρθρο 2 στο Διαδίκτυο και η οργάνωση της αναζήτησης πληροφοριών πραγματοποιείται με την επιφύλαξη των κανόνων για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Δεν αναρτώνται πράξεις, στις οποίες περιλαμβάνονται ευαίσθητα δεδομένα προσωπικού χαρακτήρα, όπως αυτά ορίζονται στην κείμενη νομοθεσία.

ΕΥΑΙΣΘΗΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΕ ΗΛΕΚΤΡΟΝΙΚΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ, ΔΙΚΤΥΑ ΚΑΙ ΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ

1. Οι κωδικοί πρόσβασης ΔΕΝ ΠΡΕΠΕΙ να βρίσκονται σε εμφανή ή κοντινά μέρη του υπολογιστή ή πάνω στην οθόνη ή κάτω από το πληκτρολόγιο κλ. Επίσης απαγορεύεται να δίνονται σε τρίτους, και όταν οι υπάλληλοι αποχωρούν να απενεργοποιείται ο κωδικός τους.
2. Κατά την είσοδο στο λειτουργικό σύστημα ενός Η/Υ, που συνήθως είναι Windows XP,7 ή 10, πρέπει να χρησιμοποιούμε κωδικούς πρόσβασης είτε ατομικά, είτε ανά γραφείο ή κλινική. Στις διοικητικές υπηρεσίες είναι προτιμητέο να υπάρχουν ατομικοί κωδικοί ενώ στα εργαστήρια, ΤΕΠ και κλινικές ανά εργαστήριο και κλινική είναι πιο πρακτικό και θέλει λιγότερους πόρους, αλλά απόφαση του Νοσοκομείου τελικά, τι πολιτική θα ακολουθήσει.
3. Όταν κάνουμε χρήση ηλεκτρονικού ταχυδρομείου(e-mail), θα πρέπει να είμαστε ιδιαίτερα προσεκτικοί σε e-mail που έχουν άγνωστο αποστολέα, ή δεν έχουν θέμα, ή έχουν συνημμένο αρχείο αγνώστου τύπου, ή μας παραπέμπουν στο να ανοίξουμε μια άγνωστη ιστοσελίδα μέσω ενός link. Στις παραπάνω περιπτώσεις θα πρέπει άμεσα να διαγράφεται το e-mail αυτό. Σε περιπτώσεις που θέλουμε να κοινοποιήσουμε σε άλλους κάτι, θα πρέπει να κάνουμε κρυφή κοινοποίηση ώστε να μην εμφανίζονται τα e-mails όλων σε όλους τους αποδέκτες, ιδιαίτερα όταν το e-mail είναι της μορφής Ονοματεπώνυμο@domain name. Τέλος, όταν θέλουμε να στείλουμε ένα συνημμένο αρχείο που περιλαμβάνει προσωπικά δεδομένα, πρέπει να το κλειδώνουμε με κωδικό, κρυπτογραφώντας το πρώτα. Αυτό για το Office γίνεται από το κεντρικό μενού, πάνω αριστερά, με την επιλογή Προετοιμασία και μετά Κρυπτογράφηση Εγγράφου. Μετά θα πρέπει να πείτε τον κωδικό με κάποιο τρόπο σε αυτόν που θα το ανοίξει.

4. Πρέπει να γίνεται χρήση firewall και antivirus σε έναν Η/Υ. Το Νοσοκομείο μας, έχει διπλή προστασία κατά την περιήγηση στο διαδίκτυο, με τη χρήση κεντρικού hardware Firewall και κεντρικού antivirus προγράμματος για τον έλεγχο κακόβουλων προγραμμάτων και αποφυγή σελίδων πορνογραφικού ή άλλου παράνομου περιεχομένου. Όλες οι ενέργειες στο διαδίκτυο καταγράφονται και κρατούνται σε αρχείο για μήνες στο Firewall ακόμα και για τους χρήστες του Wi-Fi. Στο σπίτι τη δουλειά την κάνει ένα ενσωματωμένο στο λειτουργικό σύστημα firewall και antivirus, αλλά πολύ λιγότερο αποτελεσματικό και με ελάχιστες δυνατότητες.
5. Θα πρέπει να αποφεύγεται η χρήση USB sticks και CD-ROMs ή εξωτερικών σκληρών δίσκων, ιδίως για εξαγωγή στοιχείων, παρά αν είναι για απολύτως επαγγελματική χρήση και στη φύση της δουλειάς. (πχ εξαγωγή CD-ROMs αξονικού). Στην περίπτωση χρήσης τέτοιων συσκευών ελλοχεύει πάντα ο κίνδυνος μόλυνσης του Η/Υ, και εν συνεχεία όλου του δικτύου του Νοσοκομείου, οπότε μόνο αν είναι απολύτως απαραίτητη πρέπει να γίνεται η χρήση.
6. Σε περίπτωση αδράνειας του Η/Υ πάνω από ένα λογικό χρονικό διάστημα θα πρέπει να κλειδώνει ο Η/Υ και να ζητείται εκ νέου κωδικός για πρόσβαση. Το ίδιο θα πρέπει να συμβαίνει και σε εφαρμογές που έχουν να κάνουν με βάσεις δεδομένων.
7. Όσο περισσότερα ψηφιοποιούνται τα δεδομένα, τόσο πιο «εύκολη» είναι η διαδικασία προστασίας τους, για αυτό είναι απαραίτητο κάθε εργαζόμενος να βοηθήσει ώστε να μηχανογραφηθεί όσο περισσότερο γίνεται ο τρόπος δουλειάς του.

8. Σε όλες τις βάσεις δεδομένων που τηρούνται θα πρέπει να υπάρχουν ατομικοί κωδικοί πρόσβασης και να γίνεται επαρκής παρακολούθηση και καταγραφή των ενεργειών του χρήστη. Οι βάσεις δεδομένων στο σύνολό τους θα πρέπει να είναι κρυπτογραφημένες για μέγιστη ασφάλεια, τουλάχιστον στις περιπτώσεις που αυτό είναι τεχνικά εφικτό.
9. Στους χρήστες των Η/Υ δεν θα πρέπει να δίνεται η δυνατότητα από τους διαχειριστές εγκατάστασης προγραμμάτων, είτε μεταβολών στις βασικές παραμέτρους ασφάλειας του λειτουργικού συστήματος, και θα πρέπει ανά τακτικά χρονικά διαστήματα να ελέγχεται αν τηρείται αυτό από τους χρήστες, διότι δυστυχώς υπάρχουν προγράμματα που εγκαθίστανται με δικαιώματα χρήστη. Οι χρήστες θα πρέπει να αποφεύγουν αυστηρά να εγκαθιστούν προγράμματα και ιδίως απομακρυσμένης πρόσβασης και διαχείρισης όπως πχ το Teamviewer. Αν για έκτακτο λόγο αυτό γίνει ,πρέπει άμεσα να απεγκαθίστανται μετά την έκτακτη αυτή χρήση.
10. Φωτοαντιγραφικά, fax και εκτυπωτές θα πρέπει να προστατεύονται με τον καλύτερο δυνατό τρόπο από προσπάθεια χρήσης τους για παράνομη αντιγραφή προσωπικών δεδομένων ασθενών.

11. Πρέπει να κρατείται αντίγραφο ασφαλείας (backup) σε αρχεία ή βάσεις δεδομένων που θεωρούνται σημαντικά και περιέχουν προσωπικά δεδομένα. Στους προσωπικούς υπολογιστές τα αρχεία είναι ευθύνη των χρηστών να τα κρατάνε backup εκτός αυτών που βρίσκονται στους κοινόχρηστους φακέλους που έχει δημιουργήσει το Τμήμα Πληροφορικής, όπου είναι υπεύθυνο το Τμήμα Πληροφορικής για την ασφάλειά τους.

Οι κεντρικές βάσεις δεδομένων των πληροφοριακών συστημάτων του Νοσοκομείου κρατούνται backup σε σκληρούς δίσκους, σε ειδικές αποσπώμενες κασέτες, και σε ένα απομακρυσμένο σημείο του Νοσοκομείου για λόγους ασφαλείας. Επίσης υπάρχει και δεύτερος server που λειτουργεί παράλληλα με τον πρωτεύον για να σηκωθούν το συντομότερο δυνατόν όλες οι υπηρεσίες που αυτός προσφέρει.

Το Νοσοκομείο διαθέτει πολύ ψηλό επίπεδο ασφαλείας και διαθεσιμότητας των προσωπικών δεδομένων σε κεντρικό επίπεδο. Σε επίπεδο πριζών δικτύου υπάρχει ασφάλεια σε επίπεδο MAC address ώστε να μην μπορούν να τοποθετηθούν σε κενές πρίζες άλλα δικτυακά μηχανήματα υποκλοπής δεδομένων. Επίσης διαχωρίζονται σε επίπεδο VPN το εσωτερικό δίκτυο και το Wi-Fi ώστε να μην μπορεί να γίνει ανταλλαγή δεδομένων μεταξύ των δύο.

Το Computer Room έχει δικό του σύστημα πυρανίχνευσης και πυρασφάλειας όπως και ανίχνευσης της υγρασίας. Η πρόσβαση στο χώρο του Computer Room θα πρέπει να είναι απολύτως ελεγχόμενη με πόρτα ασφαλείας και κάρτες πρόσβασης, πιθανόν ακόμα και με κάμερα ελέγχου κατά τις ώρες εκτός ωραρίου του προσωπικού του Τμήματος.

Τέλος , θα πρέπει να υπάρχει δεύτερος ξεχωριστός, κατάλληλα διαμορφωμένος χώρος για την τοποθέτηση του δευτερεύοντος server ώστε σε περίπτωση φωτιάς ή πλημμύρας να υπάρχει η δυνατότητα να λειτουργήσει το σύστημα σε σχετικά μικρό χρονικό διάστημα.