Ασφαλεια και Ελεγχος Νοσοκομειακων Πληροφοριακων Συστηματων

- ΒΑΓΙΑ ΑΙΚΑΤΕΡΙΝΗ
- ΒΑΣΙΛΕΙΟΥ ΑΝΑΣΤΑΣΙΟΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ ΕΒΔΟΜΟ
ΤΕΧΝΙΚΟ ΜΕΡΟΣ

ΕΙΣΑΓΩΓΗ

Θέματα που αναπτύσσονται στην πτυχιακή εργασία είναι :

Στο πρώτο κεφάλαιο δίνεται ο ορισμός της Ασφάλειας ενός πληροφοριακού συστήματος ενώ ταυτόχρονα αναλύεται η ύπαρξη της Αναγκαιότητας της Ασφάλειας και παράλληλα δίνεται έμφαση στην Αξία που έχει η κάθε είδους πληροφορία. Επίσης παρουσιάζονται οι επιπτώσεις από την έλλειψη Ασφάλειας ,που πιθανών να προκύψουν, γίνεται αναφορά στις απειλές που δέχεται ένα πληροφοριακό σύστημα και τέλος παρουσιάζουμε τον ρόλο που διαδραματίζει ο ανθρώπινος παράγοντας και πως επηρεάζει την Ασφάλεια ενός πληροφοριακού συστήματος. Στο δεύτερο κεφάλαιο παρουσιάζεται και αναλύεται το θεσμικό πλαίσιο μέσα στο όποιο λειτουργεί ένα Πληροφοριακό Σύστημα Υγείας καθώς και τα αίτια της ιδιαίτερης σημασίας των Ιατρικών Πληροφοριακών Συστημάτων. Στο τρίτο κεφάλαιο εξετάζονται οι λειτουργίες του HARDWARE-SOFTWARE. Αναλύεται η ασφάλεια του Λειτουργικού Συστήματος και της Βάσης Δεδομένων, στοιχεία τα οποία αποτελούν σημαντικές συνιστώσες για την ασφάλεια ενός πληροφοριακού συστήματος. Στο τέταρτο κεφαλαίο αναφέρονται τα εναλλακτικά κέντρα πληροφορικής και η αναγκαιότητα ύπαρξης ενός πλήρους σχεδίου έκτακτης ανάγκης. Στη συνέχεα αναφέρονται οι κίνδυνοι και τα μέτρα που πρέπει να ληφθούν για να καλυφθούν επαρκώς η φυσική κα λογική ασφάλεια των πληροφοριακών συστημάτων και η ασφάλεια των λοιπών δικτύων του περιφερειακού και βοηθητικού εξοπλισμού. Στο κεφάλαιο πέμπτο γίνεται μια λεπτομερής αναφορά στα διάφορα είδη *δικτύων* που υπάρχουν και την ασφάλεια που παρέχουν όταν γίνεται διακίνηση *Ιατρικών Πληροφοριών* οι οποίες χαρακτηρίζονται ως δεδομένα *υψηλής ευπάθειας*. Στο κεφάλαιο έκτο αναφέρονται **οι επιπτώσεις**, που προκύπτουν από την έλλειψη ασφάλειας και ελέγχου, στις διάφορες κατηγορίες εργασιών και υπηρεσιών που λαμβάνουν χώρα σε ένα νοσοκομείο. Στο έβδομο κεφάλαιο εχουμε το τεχνικό μέρος όπου έχει γίνει έρευνα στο νοσοκομείο Αρεταίειο για το πώς υποστηρίζεται μηχανογραφικά και ποιες προϋποθέσεις ασφάλειας τηρεί.

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

Ασφάλεια Νοσοκομειακών Πληροφοριακών Συστημάτων

Περίληψη 1ου κεφαλαίου.

Οι κίνδυνοι που απειλούν ένα πληροφοριακό σύστημα και τα στοιχεία του είναι πολλοί και έχουν διάφορες μορφές και αιτίες. Σε συνδυασμό δε με το ότι τα πληροφοριακά συστήματα γίνονται όλο και πιο πολύπλοκα, με παράλληλη αύξηση της αλληλεξάρτησης μεταξύ των στοιχείων τους, καθιστούν τα θέματα ασφάλειας και προστασίας δύσκολα. Στην παρούσα εργασία δίνεται ο ορισμός της *Ασφάλειας* ενός πληροφοριακού συστήματος, καθώς και η *Αναγκαιότητα* της ύπαρξης αυτής ενώ ταυτόχρονα αναλύεται η σημαντικότητα της *Αξίας* της πληροφορίας. Στη συνέχεια παρουσιάζονται οι *επιπτώσεις* που πιθανόν να προκύψουν από την έλλειψη ασφάλειας σε ένα πληροφοριακό σύστημα. Παράλληλα, γίνεται μια εκτενέστερη ανάλυση των *απειλών* για την ασφάλεια ενός πληροφοριακού συστήματος και τέλος δίνεται έμφαση στο ρόλο του *ανθρώπινου παράγοντα* και πως αυτός επηρεάζει την ασφάλεια ενός πληροφοριακού συστήματος.

1.1. Η έννοια της ασφάλειας πληροφοριακού συστήματος

Εξαιτίας του ρόλου που παίζει το πληροφοριακό σύστημα σε ένα νοσοκομείο είναι φυσικό να απαιτεί ασφάλεια και προστασία. Είναι δύσκολο να δώσουμε ένα ορισμό της ασφάλειας πληροφοριακού συστήματος στον οποίο να συμφωνούν όλοι. Πιστεύουμε όμως ότι ο ακόλουθος ορισμός περιγράφει όσο γίνεται καλύτερα το περιεχόμενο του όρου αυτού.

Ορισμός: ασφάλεια πληροφοριακού συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του πληροφοριακού συστήματος, αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή. Ο ορισμός αυτός παρέχει το πλεονέκτημα της άμεσης αναφοράς στα ακόλουθα βασικά στοιχεία:

I. έμφαση όχι μόνο στο πληροφοριακό σύστημα ως ολότητα αλλά και σε όλα τα επιμέρους στοιχεία του,

II. η προφύλαξη αφορά κάθε είδους απειλή (τυχαία ή σκόπιμη),

III. η ασφάλεια του πληροφοριακού συστήματος συνδέεται άμεσα τόσο με τεχνικές, διαδικασίες και διοικητικά μέτρα όσο και με ηθικοκοινωνικές αντιλήψεις, αρχές και παραδοχές,

IV. το πλαίσιο αυτό χαρακτηρίζεται από οργάνωση. Παρέχει βέβαια προφύλαξη, όμως είναι φανερό ότι αυτή δεν θα πρέπει να εμποδίζει την απρόσκοπτη λειτουργία του συστήματος. το αντικείμενο της ασφάλειας πληροφοριακών συστημάτων είναι η προστασία των αποθηκευμένων πληροφοριών που υπόκεινται επεξεργασία ή μεταφέρονται σε ηλεκτρονική μορφή, από εσκεμμένες ή τυχαίες απειλές. Οι πληροφορίες που αποκτούνται χρησιμοποιούνται για τηλεπικοινωνίες, και αποθηκεύονται σε υπηρεσίες πληροφοριακών συστημάτων.

Οι ηλεκτρονικές υπηρεσίες πληροφοριακών συστημάτων απαιτούν ασφαλή υποδομή τηλεπικοινωνιών, ασφαλή τερματικά (συμπεριλαμβανομένων των επεξεργαστών και των βάσεων δεδομένων), καθώς και ασφαλή χρησιμοποίηση. Διαχείριση των προβλεπόμενων υπηρεσιών πρέπει να είναι από μόνη της περισσότερο ασφαλής. Για αυτό η προσέγγιση της ασφάλειας πληροφοριακών συστημάτων ξεκινά από την ανάλυση των αναγκών του ατόμου ή του οργανισμού από της υπηρεσίες πληροφοριακών συστημάτων. Η πληροφορική και τα συστήματα πληροφορικής τεχνολογίας (ΠΤ) που τα υποστηρίζουν αποτελούν τον ακρογωνιαίο λίθο. Η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητά τους είναι ύψιστης σημασίας για τη γενικότερη λειτουργικότητα ενός οργανισμού. Εξαιτίας των αυξανόμενων απειλών προς την ασφάλεια πληροφοριακών συστημάτων, οι οργανισμοί αντιμετωπίζουν τέτοιου είδους απειλές από μια μεγάλη ποικιλία πηγών. Τα συστήματα ΠΤ μπορεί να αποτελέσουν στόχο μιας ευρείας κλίμακας απειλών, συμπεριλαμβανομένων απατών με χρήση Η/Υ, κατασκοπεία, σαμποτάζ, βανδαλισμό και άλλες μορφές διακοπής ή καταστροφής.

Καινούριες πηγές καταστροφών συνεχίζουν να προβάλλουν, όπως, για παράδειγμα, πολυδημοσιευμένες απειλές που έχουν προκαλέσει ιομορφικό λογισμικό και ταλαντούχα άτομα στο να εισβάλλουν σε συστήματα (hackers). Οι κίνδυνοι που διατρέχουν τα πληροφοριακά συστήματα αναμένεται να αυξηθούν ακόμη περισσότερο, με περισσότερη φιλοδοξία και αυξημένη ιδιομορφία. Συγχρόνως, οι οργανισμοί θα μπορούσαν να γίνονται περισσότερο ευάλωτοι στους κινδύνους λόγω της αυξημένης εξάρτησης από συστήματα ΠΤ και τις ανάλογες υπηρεσίες. Η ανάπτυξη των δικτύων παρουσιάζει πλέον νέες ευκαιρίες μη εξουσιοδοτημένης προσπέλασης σε υπολογιστικά συστήματα και η τάση για χρήση κατανεμημένων συστημάτων ελαττώνει το πεδίο δράσης των κεντρικών εξειδικευμένων εργαλείων/ ενεργειών της ΠΤ. Σκοπός της ασφάλειας είναι διασφάλιση της συνοχής των υπηρεσιών και ελαχιστοποίηση των απωλειών και των ανεπιθύμητων επιπτώσεων των διαρροών ή των ατυχημάτων. Η διαχείριση της ασφάλειας πληροφοριακών συστημάτων διαθέτει ένα μηχανισμό που ενεργοποιείται για τον καταμερισμό των πληροφοριών προστατεύοντας της πληροφορίες και τα πληροφοριακά πολύτιμα στοιχεία. Καθώς η ασφάλεια δεν μπορεί να είναι ολοκληρωμένη, θα πρέπει να εισάγεται πρώτα εκεί όπου θα ωφελούσε περισσότερο, μέχρι να προσεγγιστεί ένα σημείο συμβιβασμού (σε λογικά πλαίσια) μεταξύ του κινδύνου των απωλειών και του τρέχοντος κόστους. Τα αρχικά έξοδα της ασφάλειας πληροφοριακών συστημάτων είναι συνήθως τα πιο αποτελεσματικά. Αργότερα, η σχέση κόστους – αποτελεσματικότητας μειώνεται για κάθε δραχμή που ξοδεύεται, ώσπου φθάνουμε στο σημείο όπου επιπλέον βήματα επιτυγχάνονται πολύ λίγα για άπειρο κόστος. Κάθε οργανισμός πρέπει να αποφασίσει για το επίπεδο ασφάλειας που θα έπρεπε να επιτευχθεί και το κατάλληλο, ανάλογο κόστος για το σκοπό αυτό. Πάντα θα υπάρχει κάποιο κενό. Προνοώντας όμως, για κάθε ενδεχόμενο προσπαθούμε να διασφαλίσουμε ότι ακόμα και όταν από κάποια διαβολική σύμπτωση γίνει διαρροή, τουλάχιστον ο οργανισμός θα μπορέσει να επιβιώσει. Είναι απαραίτητο να ληφθούν αποφάσεις όχι μόνο για τη διαχείριση του υπολογιστικού συστήματος, αλλά σχετικά με το μέγεθος της αναγκαιότητας της ασφάλειας και των απωλειών που θα μπορούσε να επωμιστεί ο οργανισμός. Μια αναγκαία συνθήκη για να είναι δυνατή η αποτίμηση της ασφάλειας είναι ή ύπαρξη ενός συνόλου απαιτήσεων, που πρέπει να αντιστοιχούν σε κάποια θεμελιώδη χαρακτηριστικά, με την έννοια ότι κανένα από αυτά δεν πρέπει να απουσιάζει ή να αγνοηθεί. Έτσι ενώ μπορεί να δίνετε μεγαλύτερη ή μικρότερη βαρύτητα σε κάποιο από αυτά, ανάλογα με την περίπτωση, όμως όλα πρέπει να λαμβάνονται υπόψη. Τα χαρακτηριστικά που είναι κοινά αποδεκτά είναι: η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα.

- ✓ Εμπιστευτικότητα (confidentiality) σημαίνει προστασία από το να έχουν πρόσβαση μη εξουσιοδοτημένα λογικά ή φυσικά αντικείμενα (π.χ. Προγράμματα, άνθρωποι κλπ.).

- ✓ Ακεραιότητα (integrity) είναι η ιδιότητα των στοιχείων του συστήματος (κυρίως των δεδομένων) να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα. Συνέπεια της ακεραιότητας είναι κάθε αλλαγή (π.χ. του περιεχομένου των δεδομένων) να είναι αποτέλεσμα εξουσιοδοτημένης

ενέργειας, ενώ παράλληλα, μη εξουσιοδοτημένη αλλαγή να μην είναι δυνατή.

- ✓ Διαθεσιμότητα (availability) των πόρων του συστήματος είναι η ιδιότητα των πόρων αυτών να καθίστανται αμέσως προσπελάσιμοί από κάθε εξουσιοδοτημένο λογικό ή φυσικό αντικείμενο, που απαιτεί παρόμοια πρόσβαση.

Οι πληροφορίες έχουν πολλές μορφές. Μπορεί να αποθηκεύονται σε Η/Υ, να μεταδίδονται σε δίκτυα, να τυπώνονται ή να καταγράφονται σε χαρτί, και να αναφέρονται σε συζητήσεις. Από την πλευράς της ασφάλειας, κατάλληλη προστασία θα έπρεπε να εφαρμοστεί σε όλες τις μορφές των πληροφοριών, συμπεριλαμβανομένων των χαρτιών, βάσεων δεδομένων, φιλμ, μέσων προβολής, ταινιών, δισκετών, συζητήσεων και οποιασδήποτε άλλης μεθόδου που χρησιμοποιείται για μεταφορά γνώσεων και ιδεών.

1.2. Αναγκαιότητα της ασφάλειας και η αξία της πληροφορίας των Π.Σ.

Η αναγκαιότητα της ασφάλειας σε ένα πληροφοριακό σύστημα εκφράζεται με τον έλεγχο και την εκτέλεση προγραμμάτων και παρέχει υπηρεσίες χρονοδρομολόγησης, ελέγχου εισόδου-εξόδου, διαχείριση μνήμης και άλλες σχετικές. Αναλυτικά οι ιδιότητες τις οποίες πρέπει να διαθέτει ένα πληροφοριακό σύστημα είναι οι εξής:

- Ευχρηστία (usability). Το σύστημα πρέπει να είναι σχεδιασμένο με στόχο την διευκόλυνση του χρήστη.
- Γενικότητα (generality). Το σύστημα πρέπει να μπορεί να εκτελέσει ποικίλες διαδικασίες, σύμφωνα με τις ανάγκες του χρήστη.
- Αποδοτικότητα (efficiency). Το σύστημα πρέπει να λειτουργεί γρήγορα και ορθά, χρησιμοποιώντας κατά βέλτιστο τρόπο τους διατιθέμενους πόρους.
- Ορατότητα (visibility). Ο χρήστης πρέπει να γνωρίζει όσα απαιτούνται για την βέλτιστη χρήση του συστήματος.
- Ευελιξία (flexibility). Το σύστημα πρέπει να μπορεί να προσαρμόζεται σε διαρκώς μεταβαλλόμενες καταστάσεις.
- Αδιαφάνεια (opacity). Ο χρήστης πρέπει να γνωρίζει μόνο ότι είναι απαραίτητο για να διεκπεραιώσει την εργασία του.
- Ασφάλεια (security). Το σύστημα πρέπει να διαφυλάσσει τα δεδομένα ενός χρηστή από μη εξουσιοδοτημένη χρήση τους από άλλους.
- Ακεραιότητα (integrity). Οι χρήστες και τα δεδομένα τους, πρέπει να προφυλάσσονται από απρόβλεπτες μετατροπές από μη εξουσιο-

δοτημένους χρήστες. Ευκινησία (capacity). Οι χρήστες δεν πρέπει να υφίστανται άσκοπος περιορισμούς στις ενέργειές τους.

- Αξιοπιστία (reliability). Τα συστήματα πρέπει να λειτουργούν σωστά για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.

- Συντηρησιμότητα (serviceability). Πιθανά προβλήματα στη λειτουργία του συστήματος πρέπει να μπορούν να ξεπεραστούν εύκολα και γρήγορα. Διαθεσιμότητα (availability). Το σύστημα πρέπει να εξυπηρετεί τους χρήστες όσο το δυνατόν πληρέστερα για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.

1.2.1 Η αξία των δεδομένων (πληροφοριών)

Είναι σαφές ότι όλοι οι τύποι των δεδομένων που χρησιμοποιούνται από τα υπάρχοντα σήμερα πληροφοριακά συστήματα, χειρόγραφα ή αυτοματοποιημένα, δεν παρουσιάζουν την ίδια ευπάθεια. Επιπροσθέτως ορισμένοι τύποι δεδομένων είναι δυνατόν άλλοτε να χαρακτηρίζονται ως ευπαθείς και άλλοτε όχι. Είναι επίσης σαφές ότι η διαφορά της ευπάθειας διαφόρων τύπων δεδομένων δεν οφείλεται μόνο στα ιδιαίτερα χαρακτηριστικά των πληροφοριακών συστημάτων τα οποία χρησιμοποιούν τα δεδομένα, αλλά οφείλεται ακόμα επίσης στην ίδια την φύση ή την ιδιαιτερότητα των δεδομένων αυτών. Η ευπάθεια – λόγω της φύσης ή της ιδιαιτερότητας – ενός τύπου δεδομένων συσχετίζεται άμεσα και οφείλεται, κατά κύριο λόγο στην αξία των πληροφοριών που προκύπτουν από κάποια δεδομένα, όταν τα δεδομένα αυτά είναι στην κατοχή τρίτων προσώπων. Η αξία μιας πληροφορίας , που προκύπτει από κάποια δεδομένα, μπορεί να αποτιμηθεί είτε μέσω της αντιστοίχησής της με κάποια από τις τρέχουσες αξίες ενός δεδομένου κοινωνικού συστήματος (π.χ. οικονομικό όφελος, συμμετοχή σε άσκηση εξουσίας, απεξάρτηση από κάποιο σχήμα εξουσίας). Επιπλέον μπορεί να οφείλεται στις πιθανές επιπτώσεις που μπορεί να έχει η γνώση των δεδομένων αυτών, όταν είναι στην κατοχή τρίτων προσώπων ή όταν δεν είναι ακριβή ή όταν δεν είναι στην κατοχή ή στη διάθεση των προσώπων που αφορούν. Οι επιπτώσεις από τη γνώση των δεδομένων μπορούν να εκφραστούν είτε με τη στέρηση ενός προσώπου από κάποια από τα δικαιώματά του είτε με τη στέρηση του από κάποιες από τις αξίες που διαθέτει, στα πλαίσια ενός δεδομένου κοινωνικού συστήματος. Έτσι ενώ τα προγράμματα γράφονται από προγραμματιστές πληροφοριακών συστημάτων σε μια μορφή αναγνώσιμη μόνο από επαγγελματίες πληροφορικούς, οι πληροφορίες μπορούν να ερμηνευτούν άμεσα από το ευρύτερο κοινό.

Εξαιτίας της κοινής τους φύσης, οι επιθέσεις κατά των πληροφοριών είναι περισσότερο διαδεδομένες και αποτελούν πιο σοβαρό πρόβλημα από τις επιθέσεις κατά του υλικού και του λογισμικού. Έτσι τα στοιχεία των δεδομένων έχουν μεγαλύτερη δημόσια αξία από το υλικό και το λογισμικό, αφού οι άνθρωποι γνωρίζουν πως θα τα ερμηνεύσουν. Οι πληροφορίες δεν έχουν συμβατική αξία. Για το λόγο αυτό είναι δύσκολο να μετρήσουμε την αξία

τους. Όμως έχουν κόστος ίσως μετρήσιμο σύμφωνα με το κόστος της ανακατασκευής και ανάπτυξης των απολεσθέντων πληροφοριών, το οικονομικό, κοινωνικό κοκ, κόστος που σχετίζεται με την μη διαθεσιμότητά τους κατά τη διάρκεια του ανασχηματισμού τους, το οικονομικό κύρος, όταν συγκεκριμένες πληροφορίες δημοσιοποιηθούν, η απώλεια σε ό,τι αφορά την ανταγωνιστικότητα όταν συμβεί κάποια διαρροή πληροφοριών στους ανταγωνιστές.

1.2.2 Επικαιρότητα των πληροφοριών

Η αξία κάποιων πληροφοριών μπορεί να είναι υψηλή, αλλά μερικά στοιχεία τους είναι σημαντικά μόνο για ένα συγκεκριμένο χρονικό διάστημα. Από τη μελέτη της ασφάλειας πληροφοριών προκύπτει η αρχή της επικαιρότητας (principle of timeliness) της ασφάλειας υπολογιστικών συστημάτων. Σύμφωνα με την αρχή αυτή, τα μέρη ενός υπολογιστικού συστήματος, πρέπει να προστατεύονται μέχρι να χάσουν την αξία τους. Επιπλέον τα αντικείμενα που έχουν μικρό κύκλο ζωής θα πρέπει να προστατεύονται με μέτρα προστασίας που είναι αποτελεσματικά μόνο για αντίστοιχο μικρό χρονικό διάστημα.

1.3. Μορφές απειλών

Η ασφάλεια υπολογιστικών συστημάτων προστατεύει τον Η/Υ και οτιδήποτε έχει σχέση με αυτόν – το κτίριο, τα τερματικά και τους εκτυπωτές, την καλωδίωση τους δίσκους και τις ταινίες. Κυρίως όμως προστατεύει τις πληροφορίες που είναι αποθηκευμένες σε ένα υπολογιστικό περιβάλλον. Για το λόγο αυτό εξάλλου η ασφάλεια υπολογιστικών συστημάτων αποκαλείται συχνά και ασφάλεια πληροφοριακών συστημάτων. Ταυτόχρονα σημαντικό ρόλο παίζει και ο ανθρώπινος παράγοντας διότι ένα πληροφοριακό σύστημα δημιουργείται από τον άνθρωπο και λειτουργεί μόνο αν συμμετέχει στη λειτουργία και ο άνθρωπος. Κατά συνέπεια υπάρχει μια στενή σχέση μεταξύ του ανθρώπινου παράγοντα και της ασφάλειας και προστασίας ενός πληροφοριακού συστήματος. Τρεις είναι οι σχέσεις εμπλοκής του ανθρώπινου παράγοντα στην ασφάλεια του πληροφοριακού συστήματος:

1) Η προφύλαξη του συστήματος από απειλές που προέρχονται από ενέργειες οφειλόμενες στον ανθρώπινο παράγοντα.

2) Ασφάλεια και προστασία του προσωπικού που εργάζεται μέσα στο σύστημα.

3) Πολλά μέτρα προφύλαξης στηρίζονται στο προσωπικό του συστήματος, άρα ο ανθρώπινος παράγοντας είναι μέσον εξασφάλισης της ασφάλειας στο πληροφοριακό σύστημα. Οι παραπάνω τρεις σχέσεις αναφέρονται σε

άμεση απευθείας εμπλοκή στα θέματα ασφάλειας και προστασίας. Για λόγους πληρότητας όμως, θα πρέπει να εξετάσουμε και τις κατηγορίες των ανθρώπων που έχουν άμεσο ή έμμεσο συμφέρον από την ύπαρξη αποτελεσματικής ασφάλειας και προστασίας. Αν και σήμερα κατασκευάζονται υπολογιστές των οποίων η αξιοπιστία πλησιάζει το 100% όμως όπως είδαμε το πληροφοριακό σύστημα δεν είναι μόνο ο Η/Υ. Επιπλέον είναι ένα σύστημα το οποίο έχει σχεδιαστεί από τον άνθρωπο, με τον άνθρωπο ως στοιχείο του, λειτουργεί με τη βοήθεια του ανθρώπου για τον άνθρωπο. Άρα το σύστημα θα πρέπει να προστατευθεί από πιθανές ενέργειες των ανθρώπων που είναι μέσα στο σύστημα, εκτός αυτού ή είναι υπεύθυνοι της δημιουργίας του.

Η πρώτη κατηγορία περιλαμβάνει το προσωπικό που εργάζεται μέσα στο σύστημα όπως χειριστές, διαχειριστές συστήματος, χρήστες. Πέντε είναι οι κύριες δραστηριότητες στις οποίες εμπλέκεται το προσωπικό αυτό: παραλαβή δεδομένων, μετατροπή τους, επεξεργασία, αποθήκευση και διανομή των αποτελεσμάτων (output του συστήματος). Στην κατηγορία αυτή θα πρέπει να ενταχθούν και όλοι όσοι είναι υπεύθυνοι για την ασφάλεια του συστήματος.

Στη δεύτερη κατηγορία ανήκουν οι εκτός συστήματος άνθρωποι που χρησιμοποιούν το σύστημα ως χρήστες ή παρέχουν υλικά και υπηρεσίες για τη λειτουργία και συντήρηση του (π.χ. συντήρηση υλικού ή λογισμικού, παροχή αναλώσιμου ή μη υλικού, παροχή ηλεκτρικού ρεύματος).

Τέλος, η τρίτη κατηγόρια περιλαμβάνει τους προγραμματιστές, αναλυτές, σχεδιαστές δικτύων και γενικά όλους όσους μετέχουν στις δραστηριότητες του κύκλου ζωής του συστήματος, από τον καθορισμό των απαιτήσεων μέχρι και τη λειτουργία και συντήρηση του συστήματος ή μιας εφαρμογής. Όλες αυτές οι ειδικότητες κύρια εξαιτίας του προνομιακού ρόλου που έχουν στην ανάπτυξη του συστήματος (η της εφαρμογής), είναι σε θέση να γνωρίζουν αρκετές λεπτομέρειες σχετικές με τον οργανισμό και τον τρόπο σχεδίασης, λειτουργίας και συντήρησής του. Επιπλέον έχουν εύκολη πρόσβαση στο σύστημα και φιλικές σχέσεις με το προσωπικό που ανήκει στο σύστημα. Όλα αυτά είναι μεν απαραίτητα εξαιτίας του ρόλου που έχουν οι ειδικότητες αυτές, όμως είναι ενδεχόμενο να χρησιμοποιηθούν για να προκληθεί ζημιά στο σύστημα. Τα κίνητρα και τα αιτία μιας ενέργειας των ανθρώπων αυτής της κατηγορίας μπορεί να οφείλεται στη τύχη (π.χ. κόπωση, έλλειψη πείρας), σε πρόθεση (προσωπικό όφελος), ή σε συνδυασμό και των δύο. Με δεδομένο ότι ο ανθρώπινος παράγοντας είναι ένα βασικό στοιχείο του πληροφοριακού συστήματος και κατ' επέκταση και του οργανισμού είναι φυσικό να απαιτείται η προστασία του. Έτσι ασφάλεια και προστασία του προσωπικού σημαίνει κατ' ελάχιστο:

1) εξασφάλιση της ψυχικής και σωματικής του ακεραιότητας,

2) προστασία από εξαναγκασμούς ή εκβιασμούς,

3) προφύλαξη από το να διαχειρίζεται δεδομένα χωρίς ειδική εξουσιοδότηση,

4) διευκόλυνση στο να διαχειρίζεται σωστά τις πληροφορίες,

5) εξασφάλιση σωστής μεταβίβασης των δεδομένων στα επιμέρους άτομα.

Στη κατηγορία του προσωπικού που θα πρέπει να προστατευθεί ανήκουν διάφορες ειδικότητες σχετικά με τη σχεδίαση, λειτουργία, συντήρηση αλλά και χρήση του συστήματος.

1.3.1. Απειλές υλικού

Η διαφύλαξη της ασφάλειας πληροφοριακών συστημάτων υπονοεί την διατήρηση των στοιχείων της ασφάλειας σε όλα τα τμήματα τους. Στο κεφάλαιο αυτό θα λάβουμε υπόψη τις απειλές της ασφάλειας του τεχνικού περιβάλλοντος του Η/Υ. Τα υπολογιστικά συστήματα είναι ευπαθή στις φυσικές καταστροφές (φωτιές, πλημμύρες). Καθώς τα φυσικά μηχανήματα είναι ορατά, είναι και ένα αρκετά απλό σημείο επίθεσης. Η κατάχρηση των Η/Υ μπορεί να γίνει με πολλούς τρόπους. Οι άνθρωποι έχουν επιτεθεί στον εξοπλισμό των Η/Υ επανειλημμένα, τυχαία ή εσκεμμένα (κλωτσώντας, αφήνοντας κάτι απρόσεκτα, δίνοντας χτυπήματα). Η κλοπή και οι καταστροφές είναι οι κύριες «τεχνικές» που χρησιμοποιούνται σήμερα. Για αυτό το είδος των κινδύνων, υπάρχει μια πληθώρα προληπτικών διαδικασιών που θα έπρεπε να υιοθετηθούν. Αυτές οι διαδικασίες ανήκουν σε διαφορετικά τμήματα της σχεδίασης και της υλοποίησης των πληροφοριακών συστημάτων.

1.3.2. Απειλές λογισμικού

Το λογισμικό μπορεί να καταστραφεί, να τροποποιηθεί, να διαγραφεί, ή να διατεθεί σε κάποιο μη εξουσιοδοτημένο άτομο δόλια ή τυχαία. Οι τρεις τύποι απειλών προς το λογισμικό είναι:

1. *Διαγραφή λογισμικού*, είναι εκπληκτικά εύκολο να διαγραφεί το λογισμικό. Για να αποφευχθεί αυτή η περίπτωση η προσπέλαση του ελέγχεται συνήθως από μια διαδικασία που ονομάζεται διοίκηση μεταβολών (configuration management).

2. *Τροποποίηση λογισμικού*, σε αυτή τη μορφή επίθεσης, ένα αναπτυσσόμενο πρόγραμμα τροποποιείται, ώστε να αποτύχει όταν τρέχει, είτε να κάνει κάποια εργασία για την οποία δεν προοριζόταν. Το λογισμικό μετατρέπεται σχετικά εύκολα. Αλλάζοντας ένα ή δύο ψηφία (bit) μπορεί να μετατραπεί το πρόγραμμα έτσι ώστε να μη τρέχει. Άλλες μορφές τροποποίησης περιλαμβάνουν:

- Λογικές βόμβες. Το πρόγραμμα μεταβάλλεται ώστε να δουλεύει σωστά τις περισσότερες φορές, αλλά αποτυγχάνει κάτω από ορισμένες

συνθήκες (π.χ. η συγκεκριμένη διαδικασία ενεργοποιείται για ειδικές μορφές δεδομένων).

- Δούρειοι ίπποι. Το πρόγραμμα αλλάζει, ώστε να δείχνει συνολικά να κάνει κάτι ενώ συγκαλυμμένα κάνει κάτι άλλο.

- Πόρτες παγίδες (trapdoors). Ένα νέο κρυφό σημείο προστίθεται στο πρόγραμμα .

- Διαρροή πληροφοριών. Η τροποποίηση του προγράμματος προκαλεί τη διαθεσιμότητα πληροφοριών σε λάθος άτομα ή προγράμματα.

3. *Κλοπή λογισμικού*. Το είδος αυτό των εισβολών σχετίζεται με τη μη εξουσιοδοτημένη αντιγραφή λογισμικού. Παρά τα ήδη διαθέσιμα τεχνικά και νομικά μέσα, δεν έχει βρεθεί μέθοδος που θα αντιμετωπίζει τη μη εξουσιοδοτημένη αντιγραφή. Πολλά βήματα γίνονται προς αυτή την κατεύθυνση παγκοσμίως, σήμερα.

1.3.3. Απειλές δικτύων

Τα δίκτυα είναι ουσιαστικά συλλογές υλικού, λογισμικού και πληροφοριών, δηλαδή των τριών θεμελιωδών χαρακτηριστικών κάθε υπολογιστικού συστήματος. Κάθε κομμάτι του δικτύου είναι ένα υπολογιστικό σύστημα με όλα τα συνηθισμένα προβλήματα ασφαλείας. Σε αυτά έρχεται το δίκτυο να προσθέσει το πρόβλημα της επικοινωνίας, μέσω ενός πολύ εκτεθειμένου μέσου, και της προσπέλασης από μακρινές τοποθεσίες μέσω πιθανών μη ασφαλών υπολογιστικών συστημάτων. Τα δίκτυα πολλαπλασιάζουν τα προβλήματα της ασφάλειας του υπολογιστικού περιβάλλοντος. Το γεγονός αυτό οφείλεται στους ακόλουθους λόγους:

- Τα δίκτυα έχουν συνδυάσει και πολλαπλασιάσει του κινδύνους που έχουν με το κάθε ένα από τα πρώην ξεχωριστά υπολογιστικά συστήματα (μεγάλα δίκτυα υπολογιστών (main frame), προσωπικοί υπολογιστές κλπ).

- Υπάρχει μια αύξηση στον αριθμό των διαύλων επικοινωνίας που πρέπει να προστατευθούν.

- Έχουν γίνει ασαφείς οι διακρίσεις μεταξύ των τμημάτων ενός οργανισμού όπου κάποτε μπορεί να ήταν κάποιος υπεύθυνος ενός Η/Υ ή ενός μόνο κατανεμημένου δικτύου, τώρα πρέπει να προσέχει ακόμη και για μια επικοινωνιακή συσσώρευση εντός της εταιρίας.

1.3.4. Απειλές λειτουργικού περιβάλλοντος

Το λειτουργικό περιβάλλον αποτελείται από δύο τμήματα: την τοποθεσία { (location) φυσικό περιβάλλον} του υπολογιστικού συστήματος και τους χρήστες που αναμειγνύονται στη λειτουργία του συστήματος. Το πρόβλημα της ασφάλειας δεν προέρχεται από το μηχάνημα αλλά από τους χρήστες του μηχανήματος, ο τρόπος με τον οποίο αντιμετωπίζουν οι χρήστες το μηχάνημα και οι ευθύνες σε ότι αφορά τη χρήση του επηρεάζουν την ασφάλεια του συστήματος. Οι χρήστες πρέπει να λαμβάνουν υπόψη τους τις πιθανές ευπάθειες που μπορεί να προκύψουν από την επεξεργασία κειμένου και δεδομένων σε ένα Η/Υ (κάτι που δεν συμβαίνει συχνά). Ανεξάρτητα από το επίπεδο της ασφάλειας που εφαρμόζεται σε ένα σύστημα, μόνο εάν οι χρήστες ακολουθούν συγκεκριμένους κανόνες, αξιοποιούνται τα μέτρα ασφαλείας. Για παράδειγμα, ένα εκτυπωμένο κείμενο μπορεί να περιέχει ευαίσθητες πληροφορίες και όταν βρεθεί εκτεθειμένο πάνω σε ένα γραφείο ή δεν σκιστεί πριν πεταχτεί στο καλάθι των αχρήστων, μπορεί να αποτελέσει μια εύκολη και ίσως μη παρατηρήσιμη πηγή ασφαλούς ροής πληροφοριών. Επιπλέον, ένα ξεκλείδωτο ντουλάπι, όπου περιέχει ευαίσθητες πληροφορίες μπορεί να προκαλέσει ένα άτομο να το ανοίξει και να εξετάσει τα περιεχόμενά του.

1.4. Επιπτώσεις από την έλλειψη ασφάλειας σε ένα Ν.Π.Σ.

Η ανάπτυξη πληροφοριακών συστημάτων για το χώρο της υγείας βασίζεται κυρίως στη χρήση συνήθων τεχνικών της τεχνολογίας λογισμικού (sadt, case). Με την χρήση των τεχνικών αυτών έχουν σχεδιαστεί με επιτυχία τόσο διαχειριστικά (διοικητικά οικονομικά) πληροφοριακά συστήματα όσο και ιατρικά πληροφοριακά συστήματα, δηλαδή συστήματα σχεδιασμένα για την παροχή αμιγώς ιατρικών υπηρεσιών (όπως έμπειρα συστήματα ιατρικών διαγνώσεων, πληροφοριακά συστήματα για την τήρηση και αξιοποίηση του ιατρικού ιστορικού των ασθενών, πληροφοριακά συστήματα για την επιλογή φαρμακοθεραπείας με βάση το ιστορικό). Μια από τις βασικές διαφορές των δύο αυτών κατηγοριών πληροφοριακών συστημάτων εντοπίζεται στις πιθανές περιπτώσεις που μπορεί να έχει η μη ασφαλής λειτουργία τους στους εξής παράγοντες:στο επίπεδο και στη ποιότητα της παρεχόμενης περίθαλψης, στην πορεία της υγείας των ασθενών, αλλά και του κοινωνικού συνόλου γενικότερα, στα δικαιώματα των ασθενών (ως ασθενών ή ως πολιτών γενικότερα).

Έτσι: η ανασφαλής λειτουργία, η διακοπή της λειτουργίας ή η λειτουργία με λαθεμένα ή ελλιπή δεδομένα ενός διαχειριστικού πληροφοριακού συστήματος, δεν είναι πιθανό να έχει κάποια αξιοσημείωτη επίπτωση στην υγεία ενός ασθενή – μπορεί όμως να έχει στην περίπτωση που προκύψει καθυστέρηση στην προμήθεια ενός εξειδικευμένου σκευάσματος. Η δυσλειτουργία αυτή είναι πιο πιθανό να οδηγήσει σε βλάβη των δικαι-

ωμάτων του ασθενή (η μη έγκυρη ενημέρωση του ασφαλιστικού φορέα του ασθενή μπορεί να προκαλέσει τη μη εκπλήρωση των υποχρεώσεων του φορέα προς αυτόν). Οι ανασφαλής λειτουργία, η διακοπή της λειτουργίας ή λειτουργία με χρήση λαθεμένων ή ελλιπών δεδομένων ενός ιατρικού πληροφοριακού συστήματος, είναι πολύ πιθανό να οδηγήσει στην υποβάθμιση ή τη διακοπή των παρεχομένων υπηρεσιών υγείας, με αρνητικές επιπτώσεις στην υγεία των ασθενών. Επίσης, η γνωστοποίηση σε αναρμόδια πρόσωπα ιατρικών δεδομένων που αφορούν την κατάσταση της υγείας ενός ασθενή, στερεί από τον ασθενή το δικαίωμα του απαραβίαστου, της προσωπικής του ζωής. Συνεπώς, τα πληροφοριακά συστήματα, των οποίων η εξασφάλιση επείγει, είναι τα ιατρικά πληροφοριακά συστήματα. Η μη ύπαρξη ασφαλών πληροφοριακών συστημάτων είναι δυνατόν να προκαλέσει:οικονομική απώλεια, διακοπή εργασιών, απώλεια καλής φήμης ή θέλησης, αποτυχία σεβασμού νομικών υποχρεώσεων, παραβίαση προσωπικής ζωής, κίνδυνο στην ατομική ασφάλεια, αποκάλυψη ευαίσθητων πληροφοριών.

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

Ιδιαιτερότητες που Παρουσιάζουν τα Νοσοκομειακά Πληροφοριακά Συστήματα σε Σχέση με την Ασφάλεια.

Περίληψη 2ου Κεφαλαίου.

Το πρόβλημα της ασφάλειας είναι πολύ σημαντικό στα σύγχρονα αυτοματοποιημένα συστήματα, ιδιαίτερα δε σε αυτά που λειτουργούν σε περιβάλλοντα υψηλής ευπάθειας.

Ο καθορισμός των απαιτήσεων ασφάλειας ενός Πληροφοριακού Συστήματος Υγείας ειδικότερα, κατέχει έναν πολύ σημαντικό ρόλο στην γενικότερη ασφάλεια των πληροφοριακών συτημάτων. Στο κεφάλαιο αυτό παρουσιάζεται και αναλύεται το θεσμικό πλαίσιο μέσα στο οποίο λειτοθργεί ένα Πληροφοριακων Συστημάτων Υγείας, καθώς και τα αίτια της ιδιαίτερης σημασίας των Ιατρικών Πληροφοριακών Συστημάτων.

2. Ιδιαιτερότητες που Παρουσιάζουν τα Νοσοκομειακά Πληροφοριακά Συστήματα σε Σχέση με την Ασφάλεια.

Είναι σαφές ότι όλοι οι τύποι των δεδομένων που χρησιμοποιούνται από τα υπάρχοντα σήμερα πληροφοριακά συστήματα, χειρόγραφα ή αυτοματοποιημένα, δεν παρουσιάζουν την ίδια ευπάθεια. Επιπροσθέτως, ορισμένοι τύποι δεδομένων είναι δυνατόν άλλοτε να χαρακτηρίζονται ως ευπαθείς και άλλοτε όχι. Είναι, επίσης σαφής, ότι η διαφορά της ευπάθειας διαφόρων τύπων δεδομένων δεν οφείλεται μόνο στα ιδιαίτερα χαρακτηριστικά των Π.Σ. τα οποία χρησιμοποιούν τα δεδομένα, αλλά οφείλεται, επίσης και στην ίδια τη φύση ή την ιδιαιτερότητα των δεδομένων αυτών.

Η ευπάθεια -λόγω της φύσης ή της ιδιαιτερότητας- ενός τύπου δεδομένων συσχετίζεται άμεσα και οφείλεται, κατά κύριο λόγο, στην αξία των πληροφοριών που προκύπτουν από κάποια δεδομένα, όταν τα δεδομένα αυτά είναι στην κατοχή τρίτων προσώπων. Είναι δυνατόν, μάλιστα να εντοπιστούν ορισμένα χαρακτηριστικά του συστήματος αυτού, τα οποία σχετίζονται άμεσα και καθορίζουν την ευπάθεια κάθε τύπου δεδομένων. Έτσι, η χρονική και τοπική συγκυρία, το συγκεκριμένο πρόσωπο που αφορούν τα δεδομένα, καθώς και ο ρόλος και η θέση του στο δεδομένο κοινωνικό σύνολο, το σύστημα αξιών του κοινωνικού αυτού συνόλου και ο βαθμός διήθησης της τεχνολογίας σε αυτό, είναι ορισμένοι από τους παράγοντες που επηρεάζουν την ευπάθεια των δεδομένων. Η ευπάθεια των δεδομένων μπορεί, πιο συγκεκριμένα, να χαρακτηριστεί με δυο τρόπους:

1. Η ευπάθεια ορισμένων τύπων δεδομένων που είναι ανεξάρτητη από το Π.Σ. στο οποίο χρησιμοποιούνται τα δεδομένα αυτά, ορίζεται ως εγγενής ευπάθεια στα πλαίσια ενός συγκεκριμένου κοινωνικού συστήματος.

2. Η ευπάθεια ορισμένων τύπων δεδομένων που είναι ανεξάρτητη από το Π.Σ. στο οποίο χρησιμοποιούνται και η οποία ισχύει για όλα τα μέλη του κοινωνικού συνόλου ορίζεται ως συνολική και εγγενής ευπάθεια στα πλαίσια ενός συγκεκριμένου κοινωνικού συστήματος.

Η συνολική και εγγενής ευπάθεια είναι αυτή που προκαλεί θεσμικές και κοινωνικές παρεμβάσεις είτε υπό τη μορφή νόμων είτε υπό τη μορφή κανόνων δεοντολογίας. Έτσι, η ευπάθεια αυτή ανακλάται στο σύνολο σχεδόν των θεσμικών ρυθμίσεων που αφορούν στη προστασία των δικαιωμάτων του πολίτη (π.χ. μυστικότητα της ψήφου, νόμοι για την προστασία του επαγγελματικού απόρρητου ορισμένων επαγγελμάτων, σχέδιο νόμου για την προστασία του πολίτη από την επεξεργασία των προσωπικών πληροφοριών κ.λ.π.). Επί προσθέτως, η συνολική και εγγενής ευπάθεια ορισμένων τύπων δεδομένων είναι αυτή που καθορίζει ότι τα δεδομένα αυτά -αποτελώντας ακρότατα στιγμιότυπα των ευπαθών τύπων δεδομένων- χρήζουν ιδιαίτερης προστασίας.

Τα δεδομένα που αφορούν τις πολιτικές και φιλοσοφικές αντιλήψεις και απόψεις, την κατάσταση της σωματικής και ψυχικής υγείας και τη συνδικαλιστική δράση ενός πολίτη, είναι ευρύτατα αποδεκτά ως συνολικά και εγγενώς ευπαθή δεδομένα. Από αυτά, μόνον τα δεδομένα που αφορούν τη σωματική και ψυχική υγειά έχουν αξιοποιηθεί -με κοινωνικά αποδεκτό τρόπο- από αυτοματοποιημένα Π.Σ. Υπάρχουν, δε, βάσιμες ενδείξεις ότι η αξιο-

ποίηση τους αυτή θα συνεχιστεί με αυξανόμενο ρυθμό και στο άμεσο μέλλον, τόσο στις τεχνολογικά προηγμένες, όσο και στις αναπτυσσόμενες χώρες. Άρα, τα δεδομένα που αφορούν στη σωματική και ψυχική υγειά ενός πολίτη είναι τα μόνα που συγκεντρώνουν τις εξής ιδιότητες:

-Αποτελούν συνολικά και εγγενώς ευπαθή δεδομένα, άρα ακρότατο στιγμιότυπο δεδομένων προς προστασία και εξασφάλιση.
-Αποτελούν δεδομένα τα οποία χρησιμοποιούνται ευρέως από αυτοματοποιημένα Π.Σ. και των οποίων η αξιοποίηση διευρύνεται διαρκώς.
-Αποτελούν δεδομένα των οποίων η αξιοποίηση συναντά τη γενική αποδοχή του κοινωνικού συνόλου, παρόλη τη δεδομένη ευπάθεια τους.
-Αποτελούν την πρώτη ύλη για την εφαρμογή της Ιατρικής επιστήμης, θεμελιώδες γνώρισμα της οποίας είναι η επιτακτική ανάγκη λήψης αποφάσεων υπό συνθήκες αβεβαιότητας.

Συνεπώς, όταν ένα Π.Σ. χρησιμοποιεί αυτόν τον τύπο δεδομένων, τότε το τεχνολογικό περιβάλλον του χαρακτηρίζεται ως περιβάλλον υψηλής ευπάθειας.

2.1. Καθορισμός απαιτήσεων ασφάλειας ενός Π.Σ.Υ.

2.1.1. Αφαιρετική προσέγγιση

Ως συνολικά και εγγενώς ευπαθείς οι ιατρικές πληροφορίες χαρακτηρίζονται ως χρήζουσες προστασίας και προστατεύονται με ειδικές ρυθμίσεις, πριν ακόμη αυτοματοποιηθούν τα Π.Σ. του χώρου της υγείας. Οι προστατευτικές αυτές ρυθμίσεις περιλαμβάνουν προβλέψεις τόσο δεοντολογικού χαρακτήρα (π.χ. όρκος του Ιπποκράτη),όσο και θεσμικού χαρακτήρα (π.χ. προστασία του επαγγελματικού απόρρητου).

Η αυτοματοποίηση των Π.Σ. κατέστησε επιτακτικότερο το ζήτημα της προστασίας του εμπιστευτικού χαρακτήρα των ιατρικών πληροφοριών, δεδομένου ότι με τη αυτοματοποίηση:

-Διευκολύνεται σημαντικά η ταχεία επεξεργασία μεγάλου όγκου πληροφοριών. Συνεπώς, η επίφαση της εμπιστευτικότητας των ιατρικών πληροφοριών που στηριζόταν στους μεγάλους όγκους των ιατρικών αρχείων και στην αντικειμενική αδυναμία επεξεργασίας τους σε εύλογα χρονικά διαστήματα, δεν υφίσταται πλέον.

-Διευκολύνεται σημαντικά η λήψη αποφάσεων που βασίζονται στον έλεγχο απλών ή πολύπλοκων λογικών συνδυασμών μεταξύ ιατρικών μόνον ή ιατρικών και άλλων πληροφοριών. Συνεπώς η επίφαση της εμπιστευτικότητας των ιατρικών πληροφοριών, που στηρίζονταν στην αδυναμία χειρόγραφου ελέγχου υποθέσεων, δεν υφίσταται πλέον.
-Διευκολύνεται σημαντικά ο συνδυασμός δυο ή περισσοτέρων αρχείων, τα οποία εξυπηρετούν διαφορετικούς σκοπούς, για να γίνει συνδυασμένη επεξεργασία των πληροφοριών που περιέχουν. Συνεπώς, η επίφαση της

εμπιστευτικότητας των ιατρικών πληροφοριών που στηριζόταν στο φυσικό διαχωρισμό μεταξύ αρχείων ιατρικών πληροφοριών ή μεταξύ αρχείων ιατρικών πληροφοριών και αρχείων που περιέχουν πληροφορίες που έχει νόημα να συνδυασθούν με ιατρικές, δεν υφίσταται πλέον.

-Διευκολύνεται σημαντικά η δυνατότητα διασύνδεσης μεταξύ Π.Σ. που λειτουργούν σε διαφορετικές τοποθεσίες και για διαφορετικούς σκοπούς, προκείμενου να γίνει συνδυασμένη επεξεργασία των χρησιμοποιούμενων πληροφοριών. Συνεπώς η επίφαση της εμπιστευτικότητας των ιατρικών πληροφοριών που στηριζόταν στο φυσικό διαχωρισμό και στην τήρηση σε διαφορετικές τοποθεσίες των αρχείων ιατρικών πληροφοριών ή των αρχείων που τηρούν πληροφορίες που έχει νόημα να συνδυασθούν με ιατρικές, δεν υφίσταται πλέον.

Τα συμπεράσματα που προκύπτουν από τις διαπιστώσεις αυτές είναι:

1. Η αυτοματοποίηση της επεξεργασίας των ιατρικών πληροφοριών δε δημιούργησε νέους κινδύνους, απλώς μεγιστοποίησε τους ήδη υπάρχοντες και κατέστησε τις πληροφορίες αυτές περισσότερο ευάλωτες.
2. Η μεγιστοποίηση των ήδη υπαρχόντων κινδύνων μπορεί να δημιουργήσει πρωτόγνωρες συνέπειες στα δικαιώματα των ασθενών (π.χ. στοιχεία του ιατρικού τους ιστορικού, όπως τα γενετικά χαρακτηριστικά, μπορεί να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων, τα οποία ενδέχεται να καθορίσουν το μέλλον ενός ατόμου εν άγνοια του.
3. Με την αυτοματοποίηση των Π.Σ. είναι δυνατόν να ανακύψουν ερωτήματα θεμελιώδους σημασίας, τα οποία εκ πρώτης όψεως δεν έχουν σχέση με τις μεθοδολογίες σχεδίασης των Π.Σ. (π.χ. ποια είναι η αξιοπιστία ή η χρησιμότητα των ιατρικών διαγνώσεων που βασίζονται μόνο σε αυτόματη επεξεργασία στοιχείων, αλλά με τις αρχές λειτουργίας τους.

Για την αντιμετώπιση αυτής της νέας πραγματικότητας εκτιμάται ότι απαιτείται μια συστηματική προσέγγιση, με τα εξής βασικά χαρακτηριστικά:

-Να είναι ολοκληρωμένη, λαμβάνοντας υπόψη τις απόψεις τόσο του κοινωνικού συνόλου, όσο και των εργαζομένων στο χώρο της υγείας.

-Να είναι πολυδύναμη, λαμβάνοντας υπόψη τη διεθνή εμπειρία και πρακτική.

-Να είναι πολυδιάστατη, συνδυάζοντας τεχνικά μέτρα, προτείνοντας θεσμικές ρυθμίσεις και προωθώντας και υποστηρίζοντας τις υπάρχουσες κοινωνικές τάσεις και προδιαθέσεις.

Στην προσέγγιση αυτή, για να προστατευτεί ενα Π.Σ.Υ., χρειάζονται οι εξής παρεμβάσεις:

-Να καταγράφει η άποψη των εργαζόμενων στο χώρο της υγείας, που σχετίζεται με θέματα ασφάλειας Π.Σ.Υ., προστασίας του ιατρικού απόρρητου, καθώς και εξασφάλισης των δικαιωμάτων των ασθενών (προϋπόθεση της ολοκληρωμένης προσέγγισης).

-Να αναλυθούν οι απόψεις που καταγράφηκαν, να συγκριθούν με την υπάρχουσα διεθνή εμπειρία και πρακτική και να διατυπωθούν τα βασικά συμπεράσματα που προέκυψαν. Στα πλαίσια αυτά θα γίνει και μια επίδειξη της χρησιμότητας και της άμεσης εφαρμοσιμότητας των συμπερασμάτων αυτών (προϋπόθεση της πολυδύναμης και ολοκληρωμένης προσέγγισης).

-Να διατυπωθούν οι γενικές αρχές που πρέπει να διέπουν τη λειτουργία ενός Π.Σ., για να είναι αυτό ασφαλές.

-Να συγκροτηθεί ένας Κώδικας Δεοντολογίας ο οποίος πρέπει να διέπει τη συγκεκριμένη επαγγελματική κοινότητα.

-Να περιγραφεί η τεχνική παρέμβαση που απαιτείται για την ανάπτυξη και τη λειτουργία Ασφαλών Π.Σ.Υ. (ΑΠΣΥ)(προϋπόθεση της πολυδιάστατης προσέγγισης).

Οι ενέργειες και παρεμβάσεις αυτές θα παρουσιασθούν και θα αναλυθούν μετά από την παρουσίαση και της λειτουργικής προσέγγισης.

2.1.2. Λειτουργική προσέγγιση

Η ανάπτυξη ενός Π.Σ.Υ. συντελείται σε ένα πολύπλοκο περιβάλλον, το οποίο χαρακτηρίζεται από τη συνύπαρξη πολλών παραγόντων, όπως του καθήκοντος προς τον άνθρωπο, της τεχνολογίας στην υπηρεσία του ανθρώπου, καθώς και των ιδιαιτεροτήτων και των περιορισμών του ευρύτερου κοινωνικού-οικονομικού περίγυρου κλπ. Συνεπώς, κάθε παρέμβαση στο χώρο των Π.Σ.Υ. πρέπει να λαμβάνει υπόψη της τις παραμέτρους αυτές και να εκτιμά την πιθανή αλληλεπίδραση τους.

Η ανάπτυξη και η λειτουργία Α.Π.Σ.Υ. αποτελεί μια από τις παρεμβάσεις που έχει αποφασιστικό χαρακτήρα. Αποσκοπεί στην αποτελεσματική αξιοποίηση της πληροφορικής, με παράλληλη εξασφάλιση των δικαιωμάτων των ασθενών και με ταυτόχρονη υπέρβαση των αντιφάσεων που υφίστανται μεταξύ των στόχων αυτών, αντιφάσεων που δημιουργεί το κοινωνικό-οικονομικό περιβάλλον.

Εξαιτίας της πολυπλοκότητας του περιβάλλοντος των Π.Σ.Υ., η ανάπτυξη και η λειτουργία Α.Ι.Π.Σ. πρέπει να στηριχθεί σε μια πολύπλευρη και ολοκληρωμένη παρέμβαση, η οποία περιλαμβάνει και τεχνικές και μη τεχνικές συνιστώσες.

Η τεχνική παρέμβαση στηρίζεται στην εκπόνηση μιας διευρυμένης μεθοδολογίας ανάπτυξης Π.Σ. -που δεν οριοθετείται από τους οποίους περιορισμούς κάποιας συγκεκριμένης από τις υπάρχουσες μεθοδολογίες-και που αποσκοπεί στην ανάπτυξη ασφαλών Π.Σ. σε περιβάλλοντα υψηλής ευπάθειας, ιδιαίτερα δε στην ανάπτυξη Α.Π.Σ.Υ.

Η μη τεχνική παρέμβαση στηρίζεται σε τρεις συνιστώσες:

1. Στον εντοπισμό και τη διατύπωση συγκεκριμένων-και επειχηρηματολογικά στοιχειοθετημένων -γενικών αρχών που προτείνεται να διέπουν την ανάπτυξη και λειτουργία Π.Σ. σε περιβάλλοντα υψηλής ευπάθειας- και ιδιαίτερα Π.Σ.Υ. Οι γενικές αυτές αρχές πρέπει να έχουν διατυπωθεί σύμφωνα και με τις απόψεις των εργαζομένων στο χώρο.
2. Στην εκπόνηση ενός Κώδικα Δεοντολογίας που πρέπει να διέπει τις ενέργειες όλων όσων αποφασίζουν για την ανάπτυξη ενός Π.Σ.Υ. ή αναπτύσσουν, αναβαθμίζουν, τροποποιούν ή χρησιμοποιούν το Π.Σ.Υ.

αυτό. Ο Κώδικας αυτός υιοθετείται προαιρετικά από τους ενδιαφερομένους και αντικατοπτρίζει τις θεμελιώδεις αρχές, τις προτεραιότητες και τους περιορισμούς ενός συγκεκριμένου κοινωνικό-οικονομικού περιβάλλοντος.

3. Στην προώθηση της ευαισθητοποίησης, της ενημέρωσης και της συμμετοχής των ειδικών της Πληροφορικής, των χρηστών της τεχνολογίας, αλλά και του ευρύτερου κοινωνικού συνόλου, σε θέματα που αφορούν τα προβλήματα που προκύπτουν από την ανασφαλή ανάπτυξη Π.Σ καθώς και τις πιθανές αρνητικές επιπτώσεις της τεχνολογίας αυτής.

Οι τρεις αυτές συνιστώσες θα περιγράφουν στη συνέχεια, αφού πρώτα παρουσιασθούν τα αποτελέσματα μιας μελέτης προδιαθέσεων. Έτσι:

-θα προηγηθεί η περιγραφή των γενικών αρχών,

-θα παρατεθεί η περιγραφή του προτεινομένου Κώδικα Δεοντολογίας,

-θα περιγράφει η παρέμβαση που στοχεύει στην ενημέρωση, την ευαισθητοποίηση και τη συμμετοχή των ενδιαφερόμενων μερών.

2.2. Θεσμικό πλαίσιο

Περιγραφή των γενικών αρχών

Οι απαντήσεις στις θεμελιώδεις ερωτήσεις που προηγήθηκαν, καθώς και η λειτουργική περιγραφή ενός φορέα παροχής υπηρεσιών υγείας, με έμφαση στις διαδικασίες εξασφάλισης των υπαρχόντων Π.Σ.Υ., οδηγούν στη διατύπωση των γενικών αρχών για την ασφαλή ανάπτυξη και λειτουργία ενός Π.Σ.Υ. Οι αρχές αυτές είναι συμβατές με σειρά ανάλογων προσπαθειών που έχουν αναληφθεί στο παρελθόν, τηρουμένων των ιδιαιτεροτήτων του κοινωνικού περιβάλλοντος για το οποίο προτείνονται:

ΑΡΧΗ 1: Κώδικας Δεοντολογίας. Κάθε νοσοκομείο πρέπει να συγκροτήσει και να υιοθετήσει έναν Κώδικα Δεοντολογίας, ο οποίος θα καθορίζει τις εθιμικές αρχές που πρέπει να διέπουν την ασφαλή λειτουργία των Π.Σ. του χώρου αυτού, με ταυτόχρονο σεβασμό της ιδιωτικής ζωής κάθε ασθενή.

ΑΡΧΗ 2: Συμβατικές δεσμεύσεις. Τα καθήκοντα και οι υποχρεώσεις των εργαζομένων στα νοσοκομεία, που σχετίζονται με θέματα ασφαλείας Π.Σ.Υ., πρέπει να καθορίζονται με συμφωνία Διοίκησης Νοσοκομείου και εργαζομένου.

ΑΡΧΗ 3: Συγκρότηση φορέα προστασίας των δεδομένων. Η επίβλεψη της τήρησης των γενικών αρχών για την ασφάλεια των Π.Σ.Υ. θα πρέπει να ανατίθεται σε φορέα λειτουργικά και οικονομικά ανεξάρτητο, του οποίου η αρμοδιότητα εκτείνεται σε όλες τις υπηρεσίες του νοσοκομείου.

ΑΡΧΗ 4: Εκπαίδευση -ενημέρωση- ευαισθητοποίηση. Το προσωπικό του νοσοκομείου θα πρέπει να ενημερώνεται και να εκπαιδεύεται, τόσο σε θέματα που αφορούν την ασφάλεια των Π.Σ.Υ. όσο και σε θέματα που αφορούν την προστασία της προσωπικής ζωής των ασθενών.

ΑΡΧΗ 5: Περιορισμός των κυκλοφορούντων δεδομένων. Η κυκλοφορία των ιατρικών δεδομένων, που πραγματοποιείται για την πραγμάτωση κάποιου στόχου, θα πρέπει να είναι η ελάχιστη δυνατή.

ΑΡΧΗ 6: Διασφάλιση των δικαιωμάτων των ασθενών. Τα Π.Σ.Υ. λειτουργούν με στόχο την παροχή υπηρεσιών υγείας υψηλής ποιότητας, με ταυτόχρονο σεβασμό των δικαιωμάτων των ασθενών και του ισχύοντος θεσμικού πλαισίου.
ΑΡΧΗ 7: Διασφάλιση της ποιότητας των δεδομένων. Η ακεραιότητα και η ακρίβεια των δεδομένων που χρησιμοποιούνται στα Ι.Π.Σ. πρέπει να είναι υψηλή.
ΑΡΧΗ 8: Υποστήριξη της ιατρικής έρευνας. Τα δεδομένα που χρησιμοποιούνται για την πραγματοποίηση ιατρικής ή επιδημιολογικής έρευνας πρέπει να καθίστανται ανώνυμα και ο σκοπός της επεξεργασίας τους να μην αντίκειται προς τα ανθρώπινα δικαιώματα ή τα δικαιώματα των ασθενών.
ΑΡΧΗ 9: Τεχνικές ρυθμίσεις. Η επεξεργασία των ιατρικών δεδομένων πρέπει να γίνεται με τη συνοδεία κατάλληλων τεχνικών ρυθμίσεων που στόχο έχουν να εγγυηθούν την ασφαλή λειτουργία των Π.Σ.Υ.

2.3. Κώδικας δεοντολογίας

Η προστασία των δεδομένων συνήθως εστιάζεται ή βασίζεται σε σχετικές νομοθετικές ρυθμίσεις. Όπου δεν υπάρχουν τέτοιες ρυθμίσεις,συχνά υπάρχει μια σείρα εθιμικών κανόνων που αποτελούν -κατά κάποιο τρόπο- υποκατάστατό τους. Δε λείπουν, όμως και περιβάλλοντα όπου συνυπάρχουν θεσμικές και εθιμικές ρυθμίσεις.

Οι εθιμικές ρυθμίσεις προαιρετικού χαρακτήρα οι οποίες διέπουν τη λειτουργία ενός επαγγέλματος ή ενός επαγγελματικού χώρου, σύμφωνα με τα επικρατούντα ήθη, αποτελούν έναν Κώδικα Δεοντολογίας.

Οι κώδικες δεοντολογίας συνήθως εκπονούνται απο φορείς που εκπροσωπούν επαγγελματικές ή επιστημονικές ομάδες. Οι φορείς αυτοί συνήθως είναι διεθνείς. Στο χώρο της Πληροφορικής Κ.Δ. έχουν εκπονήσει- μεταξύ άλλων –οργανισμοί όπως η I.F.P. (INTERNATIONAL FEDERATION OF INFORMATION PROCESSING), η A.C.M. (ASSOCIATION OF COMPUTING MACHINERY).

Τα βασικά χαρακτηριστικά ενός Κώδικα Δεοντολογίας είναι ότι απευθύνεται σε μια συγκεκριμένη επαγγελματική ομάδα του πληθυσμού, ότι υιοθετείται συνήθως προαιρετικά από τα μέλη της ομάδας, ότι ανακλά τις θεμελιώδεις ηθικές αρχές, τις προτεραιότητες και τους περιορισμούς ενος συγκεκριμένου κοινωνικο-οικονομικού περιβάλλοντος και ότι πρέπει να είναι αρκετά γενικός, ώστε να καλύπτει επαρκώς το στόχο του χωρίς να απαιτείται συνεχής αναθεώρηση του και συγχρόνως αρκετά ειδικός ώστε να δίνει λύσεις σε καθημερινά προβλήματα.

Ο κώδικας δεοντολογίας που θα προταθεί στη συνέχεια αποτελεί μια απο τις προτεινόμενες μη τεχνικές συνιστώσες της παρέμβασης για την εξασφάλιση ενός Π.Σ. Προέκυψε απο συνεκτίμηση των διεθνών προσπαθειών, των αποτελεσμάτων της μελέτης προδιαθέσεων που διενεργήθηκε στον Ελληνικό χώρο, κάθως και των ιδιαιτεροτήτων του επαγγελματικού περιβάλλοντος στο οποίο απευθύνεται. Οι υποχρεώσεις που προβλέπει ο προτεινόμενος κώδικας δεοντολογίας είναι οι εξής:

1. Κοινωνική υπευθυνότητα. Ο επαγγελματίας της Πληροφορικής που εργάζεται στο χώρο της υγείας χρησιμοποιεί τη γνώση και την εμπειρία του για την προαγωγή της υγείας και της ποιότητας ζωής των ασθενών, έχει δε ηθική υποχρέωση να αξιολογεί τις πιθανές επιπτώσεις των ενεργειών του και να συμβάλλει στην ασφάλη αξιοποίηση των εφαρμογών της Πληροφορικής.

2. Προστασία της προσωπικής ζωής. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας σέβεται και προστατεύει τι απαραβίαστο της προσωπικής ζώης των ασθενών, λαμβάνει δε όλα τα κατάλληλα μέτρα για την προστασία του.

3. Επιλογή δραστηριοτήτων. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας οφείλει να χαρακτηρίζεται απο αξιοπιστία και αντικειμενικότητα στις αποφάσεις του. Οφείλει,επίσης,να σέβεται και να υπερασπίζει τον ελεύθερο προβληματισμό των συνεργατών του.

4. Επαγγελματική επάρκεια. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας οφείλει να έχει συναίσθηση της προσωπικής του ευθύνης να αναβαθμίζει συνεχώς την επαγγελματική του επάρκεια. Οφείλει, επίσης, να έχει κατανοήσει το πεπερασμένο των γνώσεών του, που αφορούν στην ευρύτατη γνωστική περιοχή της πληροφορικής.

5. Προσωπική ευθύνη. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας αναλαμβάνει προσωπική ευθύνη για τις πράξεις του. Αναλαμβάνει εργασίες μόνον όταν υπάρχουν βάσιμες ενδείξεις ότι μπορεί να ανταποκριθεί στις απαιτήσεις τους, με την απαι-τούμενη επίδοση.

6. Αυτοκριτική. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας συμβάλλει στον αντικειμενίκο έλεγχο και στην αξιολόγηση της ποιότητας των Π.Σ.Υ., στην ανάπτυξη των οποίων συμμετείχε. Τα αποτελέσματα της αξιολόγησης αυτής τα λαμβάνει υπόψη του στις μετέπειτα ενέργειες του, προκειμένου να βελτιώσει περαιτέρω την απόδοσή του.

7. Υψηλή απόδοση. Με προϋπόθεση την αμέριστη συμπαράσταση του φόρεα στον οποίο παρέχει τις υπηρεσίες του, ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας αξιοποιεί τους πόρους που του παρέχονται, ώστε να επιτυγχάνει υψηλής απόδοσης.

8. Γόνιμο εργασιακό περιβάλλον. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας επιζητεί ή δημιουργεί εργασιακό περιβάλλον υψηλής ποιότητας, προς όφελος του κοινωνικού συνόλου και του ίδιου.

9. Προώθηση της συμμετοχικότητας. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας επιδιώκει και προώθει την ευρύτερη δυνατή συμμετοχή των χρηστών στην ανάπτυξη Π.Σ.Υ., αποβλέποντας στην εξασφάλιση της ευρύτερης δυνατής κοινωνικής τους αποδεκτικότητας.

10. Προστασία της πνευματικής ιδοκτησίας. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας σέβεται τις ρυθμίσεις των κανόνων περί πνευματικής ιδιοκτησίας που αφορούν προϊόντα πληροφορικής, αναγνωρίζοντάς τα ως απόρροια πνευματικής προσπάθειας.

11. Διεθνείς νομικές ρυθμίσεις. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας σέβεται, σε βάση αμοιβαιότητας, τις υπο-

χρεώσεις που απορρέουν απο το διεθνές δίκαιο και τις διεθνείς συμβάσεις και οι οποίες αφορούν την εφαρμογή της πληροφορικής στο χώρο της υγείας.

12. Αθέμιτες ενέργειες. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας αναγνωρίζει ως αθέμιτες ενέργειες τη μη εξουσιοδοτημένη προσπέλαση ή τροποποίηση δεδομένων, προ-γραμμάτων ή Π.Σ., την παρεμβολή ή εκτέλεση προγραμμάτων ιομορφών, την αποκάλυψη εμπιστευτικών πληροφοριών ή την τροποποίηση του βαθμού διαθεσιμότητας ενος Π.Σ.

13. Μετάδοση δεδομένων. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας λαμβάνει και μεταδίδει ιατρικά δεδομένα μόνον όταν με τον τρόπο αυτό εξυπηρετείται η προαγώγη της υγείας του κοινωνικού συνόλου και δε βλάπτονται ατομικά ή συλλογικά δικαιώματα.

14. Επιλεκτική χρήση Πληροφοριών. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας δε χρησιμοποιεί πληροφορίες που θίγουν τα δικαιώματα των ασθενών, αναλαμβάνοντας συγχρόνως την υποχρέωση να δημοσιοποιήσει τους λόγους για τους οποίους πιστεύει ότι δεν εξασφαλίζονται τα δικαιώματα αυτά.

15. Αξιοποίηση γνώσης και εμπειρίας. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας αξιοποιεί την υπάρχουσα επιστημονική γνώση, που αφορά τα Π.Σ.Υ. και τις μεθοδολογίες και τεχνικές που αποβλέπουν στην εξασφάλισή τους. Συνεισφέρει δε και ο ίδιος με τη δική του γνώση και εμπειρία.

16. Συνεισφορά στην ανάπτυξη. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας αναγνωρίζει τις διαφορές που υπάρχουν ανάμεσα στο επίπεδο ανάπτυξης των Π.Σ.Υ., μεταξύ των διάφορων χωρών και συνεισφέρει στη μείωση των διαφορών αυτών.

17. Σεβασμός του περιβάλλοντος και της ποιότητας ζωής. Ο επαγγελματίας της πληροφορικής που εργάζεται στο χώρο της υγείας σέβεται το φυσικό και πολιτιστικό περιβάλλον μέσα στο οποίο ενεργεί. Η δε προαγωγή της ποιότητας ζωής, στην οποία αποβλέπει μέσω των παρεχομένων υπηρεσιών υγείας, έχει ως βάση τη διατήρηση της πολιτιστικής και φυσικής κληρονομιάς.

2.4. Αίτια της ιδιαίτερης σημασίας των ιατρικών πληροφοριακών συστημάτων.

Τα δεδομένα που αποθηκεύονται στα Π.Σ. των περισσοτέρων οργανισμών αποτελούν ιδιαίτερα πολύτιμα αγαθά. Αυτό ισχύει και για τις υπηρεσίες ιατρικής περίθαλψης. Όλα τα συστήματα επεξεργασίας πληροφοριών στο ιατροκεντρικό περιβάλλον πρέπει να προστατεύονται σε ικανοποιητικό επίπεδο από όλα τα γεγονότα που θα μπορούσαν πιθανώς να θέσουν σε κίνδυνο ιατρικές δραστηριότητες. Τα γεγονότα αυτά συμπεριλαμβάνουν ατυχήματα αλλά και δραστηριότητες που γίνονται εσκεμμένα, ώστε να προκαλέσουν δυσκολίες.

Μια πληθώρα λόγων αλλά και διαπιστώσεων από ερευνητικές παγκοσμίως -και ιδιαίτερα στην Ευρώπη μέσα από ένα πλήθος ερευνητικών

προγραμμάτων- μας προσανατόλισαν να εστιάσουμε το ενδιαφέρον μας στην ασφάλεια των ιατρικών Π.Σ. Περιληπτικά αναφέρουμε τους εξής:

Α) Τα πληροφοριακά συστήματα που εξυπηρετούν ιατρικούς σκοπούς περιέχουν πολλά δεδομένα που συνδέονται άμεσα με τους ανθρώπους, το βιοτικό τους επίπεδο και την θεραπεία τους και θεωρούνται άκρως εμπιστευτικά. Οι γνώσεις που απορρέουν από αναλύσεις στατιστικών μπορούν να οδηγήσουν σε καλύτερη περίθαλψη. Η χρήση όμως δεδομένων για στατιστικές αναλύσεις θα μπορούσε να περιοριστεί από κανόνες ιδιωτικότητας.

Β) Τα ιατρικά δεδομένα μπορούν να έχουν επιπτώσεις στην υγειά και θεραπεία των ασθενών και συνεπώς η ακεραιότητα τους είναι ουσιώδεις. Ο χρόνος ύπαρξης των δεδομένων σε ιατροκεντρικούς οργανισμούς κυμαίνεται από μερικές ώρες ως και τριάντα ή και περισσότερα χρόνια. Το γεγονός αυτό προσθέτει ένα ακόμη παράγοντα πολυπλοκότητας της διαφύλαξης της ακεραιότητας των δεδομένων κατά τη διάρκεια της ύπαρξης τους.

Γ) Συνήθως, το φυσικό περιβάλλον στα περιβάλλοντα ιατρικής περίθαλψης είναι ιδιαίτερα ανοιχτό. Σε ένα νοσοκομείο, οι άνθρωποι (ασθενείς και επισκέπτες) εισέρχονται ελεύθερα στα κτίρια και στις περιοχές όπου δεν ισχύουν ώρες επισκεπτηρίου.

Δ) Η απαιτούμενη διαθεσιμότητα των συστημάτων που σχετίζονται με την θεραπεία των ασθενών και τη φροντίδα τους είναι συχνά 24ωρες το εικοσιτετράωρο επτά ήμερες τη εβδομάδα.

Ε) Η διαχείριση των περισσοτέρων δεδομένων πρέπει να γίνεται ουσιαστικά on line γιατί τα δεδομένα πρέπει να είναι όσο το δυνατό συντομότερα διαθέσιμα για περαιτέρω θεραπεία του ασθενή (π.χ. αποτελέσματα εργαστηριακών εξετάσεων). Έχουμε δηλαδή υψηλό ποσοστό on line επεξεργασίας κινήσεων κάτι που απαιτεί υψηλό βαθμό ακεραιότητας των συστημάτων.

Στ) Τα δεδομένα μπορεί να είναι κρίσιμα για κάποια ενεργεία

Ζ) Στα ιδρύματα ιατρικής περίθαλψης η ιεραρχία των ανθρώπων που είναι υπεύθυνοι για την ασφάλεια είναι σχεδόν επίπεδη.

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

Δυνατότητες Σημερινής Τεχνολογίας.

Περίληψη 3ου κεφαλαίου.

Η ασφάλεια των πληροφοριακών συστημάτων αποτελεί γνωστική περιοχή η οποία αναδείχτηκε στην αιχμή του ενδιαφέροντος της επιστημονικής κοινότητας της πληροφορικής τα τελευταία χρόνια. Στο κεφάλαιο αυτό εξετάζονται οι λειτουργίες του *HARDWARE* δηλαδή το υλικό ενός πληροφοριακού συστήματος και πως μπορούμε να το προστατεύσουμε καθώς και του *SOFTWARE* δηλαδή το λογισμικό ενός Η/Υ, το οποίο περιλαμβάνει το *Λειτουργικό Σύστημα*, τη *Βάση Δεδομένων* και διάφορες εφαρμογές ανάλογα με τις απαιτήσεις του οργανισμού. Γίνεται εκτενέστερη ανάλυση στην ασφάλεια του λειτουργικού συστήματος και της βάσης δεδομένων, λειτουργίες οι οποίες αποτελούν σημαντικές συνιστώσες για την ασφάλεια ενός πληροφοριακού συστήματος και οριοθετούν το συνολικό πλαίσιο λειτουργίας του.

3. Δυνατότητες Σημερινής Τεχνολογίας.

Η έννοια της ασφάλειας θα πρέπει από νωρίς να απασχολήσει ένα οργανισμό ο οποίος επιπλέον θα πρέπει να καθορίσει και το επίπεδο ασφαλείας (ανάλογα με το κόστος). Τίποτα όμως δε μπορεί να εγγυηθεί ένα τέλειο σύστημα ασφαλείας. Έτσι, οι υπεύθυνοι είναι υποχρεωμένοι να μάθουν να ζουν με την πιθανότητα ότι κάτι μπορεί να συμβεί αναλαμβάνοντας το ρίσκο της αποτυχίας του συστήματος ασφαλείας. Ακόμα, πρέπει να υπάρχει υψηλός δείκτης ετοιμότητας για επαναφορά του συστήματος.

Είναι αναγκαίο οι υπεύθυνοι να δίνουν μεγάλη σημασία στην ασφάλεια των συστημάτων που επιβλέπουν και να την επιβεβαιώνουν μετά την προμήθεια κάποιου προϊόντος υλικού ή λογισμικού. Οι χρήστες από την μεριά τους, θα πρέπει να καταλάβουν τη σπουδαιότητα της προστασίας και της ασφάλειας των δεδομένων τους.

Η ασφάλεια των συστημάτων θα πρέπει να έχει την υψηλότερη δυνατή προτεραιότητα και ιδιαίτερα για εκείνα τα συστήματα που συνδέονται σε δίκτυα.

Ένα περίγραμμα ενός αποτελεσματικού τρόπου διαχείρισης του θέματος της ασφάλειας, αποτελεί η παρακάτω λίστα:

- Καθορισμός της σπουδαιότητας της ασφάλειας του όλου συστήματος και γνωστοποίηση του στοιχείου αυτού στην ανώτατη Διοίκηση.
- Προσδιορισμός των τομέων που αφορά το θέμα της ασφάλειας.
- Λίστα προτεραιοτήτων στους τομείς αυτούς.
- Εγκατάσταση συστήματος εσωτερικού ελέγχου.
- Λίστα προτάσεων για βελτιώσεις.
- Περιοδική επιθεώρηση των διαδικασιών ασφαλείας, ώστε να επιβεβαιώνεται ότι αυτές ακολουθούνται και παραμένουν αποτελεσματικές.
- ***Τρεις είναι οι βασικές περιοχές ασφαλείας που πρέπει να προσδιοριστούν:***

Α) Ασφάλεια Εξοπλισμού και Πρόσβασης σε αυτόν

Β) Ασφάλεια Επικοινωνίας

Γ) Κτιριακή και Περιβαλλοντική Ασφάλεια

3.1. Ασφάλεια εξοπλισμού και πρόσβασης.

Μόνο εξουσιοδοτημένα άτομα πρέπει να έχουν το δικαίωμα πρόσβασης στις μονάδες εισόδου και εξόδου του υπολογιστή. Οι μονάδες αυτές, καθώς και ο ίδιος ο υπολογιστής (όταν πρόκειται για κεντρικό σύστημα), μπορεί να βρίσκονται σε δωμάτια ελεγχόμενης πρόσβασης, που απαιτούν κάποιο ειδικό κλειδί ή μαγνητική κάρτα ή και συνδυασμό τους. Επιπλέον, ένας χρήστης δε μπορεί να έχει πρόσβαση σε οποιοδήποτε αρχείο δεδομένων, αλλά μόνο σε εκείνα που αφορούν τη δουλειά του. Αυτό επιτυγχάνεται με τη χρήση κωδικών από την πλευρά του χρήστη, που για λόγους αποτελεσματικότητας, πρέπει να αλλάζουν περιοδικά και οι οποίοι ονομάζονται passwords. Επίσης, η πρόσβαση του χρήστη πρέπει να ελέγχεται, έτσι ώστε κάθε χρήστης να μπορεί να έχει περιορισμένο ορίζοντα του συστήματος, τόσο σε επίπεδο εφαρμογών, όσο και σε επίπεδο λειτουργίας (μόνο διάβασμα ή γράψιμο δεδομένων).

3.1.1. Αντίγραφα ασφαλείας (BACKUP)

Η ύπαρξη αντιγράφων ασφαλείας αναφέρεται στη διαθέσιμη υποστήριξη μιας εγκατάστασης και χρησιμοποιούνται όταν ένα ή περισσότερα τμήματα του εξοπλισμού, που απαιτείται για τη φυσιολογική λειτουργία του συστήματος, αχρηστεύονται ή δυσλειτουργούν για κάποιο σημαντικό διάστημα χρόνου. Η σπουδαιότητα της ύπαρξης των αντιγράφων ασφαλείας δε μπορεί να τεκμηριωθεί με ιδιαίτερη έμφαση. Όσο όμως και αξιόπιστο να είναι ένα σύστημα, είναι καταδικασμένο κάποτε να αποτύχει και μολονότι η μέση συχνότητα τέτοιων σφαλμάτων μπορεί να προβλεφθεί, δε μπορεί να προβλεφθεί μια διακεκριμένη έμφαση λάθους. Ο σχεδιαστής του συστήματος είναι υπεύθυνος να διαβεβαιώσει ότι ο βαθμός αυτής της εμφάνισης λάθους είναι ελαχιστοποιημένος.

3.1.2. Αντίγραφα ασφαλείας υλικού

Μπορεί να εφαρμοστεί πολύ καλά χρησιμοποιώντας μια εγκατάσταση μαγνητικής ταινίας. Είναι συχνά καλό, να κρατείται μια ταινία παραπάνω, από αυτές που απαιτούνται για τη λειτουργία του συστήματος. Κατά την εμφάνιση ενός λάθους, η επαναφορά του συστήματος είναι εύκολη υπόθεση και γίνεται με τη χρήση εφεδρικών ταινιών. Όταν ένα κρίσιμο κομμάτι του υλικού δυσλειτουργεί, όπως ένας δίσκος ή ένας κεντρικός επεξεργαστής, ο αναλυτής του συστήματος και ο χρήστης πρέπει να αναπτύξουν μια διαδικασία για να αντιμετωπίσουν το σφάλμα. Αυτή η διαδικασία μπορεί να διαπραγματεύεται

την απόφαση αν το σύστημα θα λειτουργήσει σε μια άλλη μηχανή, που εκτελεί τις ίδιες δραστηριότητες ή αν θα αναπτυχθούν οι δραστηριότητες αυτές για δεύτερη φορά στην ίδια θέση. Όσο απλή και αν είναι η διαδικασία αυτή, πρέπει να έχει αναπτυχθεί πριν από την εμφάνιση του λάθους.

3.1.3. Αντίγραφα ασφαλείας δεδομένων

Αυτά παρέχουν την εγγύηση και τη βεβαιότητα απέναντι στην απώλεια των δεδομένων, που μπορεί να γίνει από δυσλειτουργία του υλικού, την αποτυχία του προγράμματος ή κάποιο άλλο ατύχημα. Ο τύπος των αντιγράφων ασφαλείας των δεδομένων εξαρτάται κατά πολύ από το μέγεθος των πρωτότυπων αρχείων.

3.1.4. Αντίγραφα συστήματος

Η συντήρηση ενός μεγάλου αρχείου σε ένα δίσκο, μπορεί να απαιτεί την εξακολούθηση της λειτουργίας του συστήματος, ακόμα και όταν ο δίσκος δε λειτουργεί σωστά. Τότε, θα πρέπει να σχεδιαστεί ένα εναλλακτικό σχήμα επεξεργασίας, το οποίο θα επιτρέπει τη συνέχιση της λειτουργίας. Στη χειρότερη περίπτωση, το σύστημα μπορεί να απαιτήσει διαδικασίες ανάκτησης για τη συνέχιση της λειτουργίας του, κατά την εμφάνιση ενός παρατεινόμενου μηχανικού λάθους.

3.1.5. Μονάδες BACKUP

Οι μονάδες που παίρνουμε backup ποικίλουν. Αρχικά, πιο διαδεδομένη μέθοδος, η οποία και σήμερα εξακολουθεί να χρησιμοποιείται, είναι η χρήση δισκετών. Όταν τα δεδομένα είναι όμως πολλά, αυτή η μέθοδος απαιτεί αφ'ενός πολύ χρόνο, λόγω της μικρής ταχύτητας μεταφοράς και των συχνών αλλαγών δισκετών, αφ'ετέρου, δεν παρέχει μεγάλη ασφάλεια.

Μια εξίσου διαδεδομένη μέθοδος είναι η χρήση ταινιών (tape streamer). Μια τέτοια συσκευή, παίρνει μαγνητικές ταινίες ή μαγνητικούς δίσκους(disk cartridges-DC), όπου αφ'ενός έχουμε πιο μεγάλες ταχύτητες, μεγάλους όγκους δεδομένων και αρκετή ασφάλεια. Το streamer μπορεί να είναι εσωτερικό ή εξωτερικό. Τα χαρακτηριστικά ενός streamer είναι τα εξής:

-Η χωρητικότητα της ταινίας ή του DC, που παίρνει τιμές από 200 MB μέχρι μερικά GB.

-Η ταχύτητα μεταφοράς κυμαίνεται συνήθως από 10 MB\λεπτό περίπου.

-Ο τύπος cartridge που χρησιμοποιείται.

-Ο τύπος σύνδεσης (interface-παράλληλος ή σειριακός).

-Passwords:Υπάρχουν κωδικοί ασφαλείας χρήσης.

Μια άλλη μέθοδος για BACKUPP είναι η χρήση μετακινούμενων δίσκων (Removable Disks). Η μέθοδος αυτή, δεν εφαρμόζεται ευρέως λόγο του πολύ υψηλού κόστους. Το κόστος σήμερα σε συστήματα BACKUP κυμαίνεται από 100.000δρχ ως 2.000.000δρχ.

3.2. Κατάσταση ελέγχου αντιγράφων ασφαλείας

-Εγγραφή Τεκμηρίωση του Συστήματος.

-Εγγραφή Τεκμηρίωση των Προγραμμάτων.

-Εγγραφή Τεκμηρίωση των Λειτουργικών Διαδικασιών.

-Ταινίες με το πηγαίο πρόγραμμα.

-Ταινίες ή πακέτα δίσκων με το Λειτουργικό Σύστημα.

-Πρωτότυπα Αρχεία Δεδομένων .Κ

-Αρχεία Αναφορών.

-Αρχεία Φορμών (Τυποποιημένων Οθόνων).

-Εγχειρίδια.

-Εγγραφή Τεκμηρίωση των καθηκόντων του προσωπικού.

-Περιγραφή της διάρθρωσης του υλικού, συμπεριλαμβανομένων και όλων των περιφερειακών μονάδων

3.3. Ασφάλεια επικοινωνίας

Η ασφάλεια επικοινωνίας πρέπει να λύσει δυο ανεξέλεγκτες καταστάσεις που αφορούν τη γραμμή επικοινωνίας:

Α)Διαρροή (άκουσμα) των πληροφοριών και των μηνυμάτων πάνω στη γραμμή επικοινωνίας.

Β)Καταγραφή της μετάδοσης με σκοπό τη μεταβολή της.

Για την ασφάλεια των αποστελλόμενων πληροφοριών χρησιμοποιούνται τεχνικές κωδικοποίησης που ονομάζονται και τεχνικές κρυπτογράφησης δεδομένων.

Στην κρυπτογράφηση δεδομένων ο κάθε χαρακτήρας του μηνύματος αντικαθιστάται από άλλους κωδικοποιημένους χαρακτήρες. Ο αποστολέας είναι εκείνος που καθορίζει τον τρόπο κωδικοποίησης(αλγόριθμο αντικατάστασης), σύμφωνα με ένα προεπιλεγμένο κλειδί. Αν κάποιος κλέψει το κρυπτογραφημένο μήνυμα, ακόμα και αν γνωρίζει τον αλγόριθμο κρυπτογράφησης, είναι πολύ δύσκολο να αποκρυπτογραφήσει το μήνυμα, επειδή δεν γνωρίζει το κλειδί.

3.4. Κτιριακή και περιβαλλοντική ασφάλεια.

3.4.1. Αντιμετώπιση καταστροφής

Ενώ μια καταστροφή σε μια εταιρεία είναι γενικά μη προβλεπόμενη, τα αποτελέσματα της είναι προβλεπόμενα. Διακοπή λειτουργίας, απώλεια εσόδων, μειωμένη ποιότητα υπηρεσιών, είναι μερικά από αυτά. Επιπλέον, υποφέρουν το εργατικό προσωπικό, οι πελάτες αλλά και οι διαχειριστές.

Παρόλο όμως που μια καταστροφή θα πρέπει να είναι στα σχέδια μιας επιχείρησης, μόνο ένα μικρό ποσοστό επιχειρήσεων διαθέτει σχέδιο αντιμετώπισης και επαναφοράς.

Ευτυχώς, οι διαχειριστές αρχίζουν να διαπιστώνουν τη χρησιμότητα ενός τέτοιου σχεδίου, και ιδιαίτερα σε επιχειρήσεις που εκτελούν καθημερινά επεξεργασία κάποιων δεδομένων.

Επειδή η ακριβείς φύση μιας καταστροφής είναι απρόβλεπτη, ο διαχειριστής της επιχείρησης, δεν πρέπει να χρησιμοποιηθεί κάποιο ειδικό σχέδιο προστασίας. Ένα τέτοιο σχέδιο, πρέπει να προβλέπει πως θα αντιμετωπισθεί μια πυρκαγιά, μια πτώση τάσης, μια τρομοκρατική ενέργεια. Ένα καλό σχέδιο προστασίας είναι εκείνο, με το οποίο μπορεί να γίνει εύκολη και γρήγορη επαναφορά όλων των κρίσιμων (σημαντικών) λειτουργιών της επιχείρησης.

3.4.2. Εμβέλεια σχεδίου προστασίας

Η εμβέλεια δηλαδή τα στοιχεία που περιλαμβάνει το σχέδιο προστασίας, είναι τα παρακάτω:

1. Προσδιορισμός του προσωπικού που θα λάβει μέρος στο σχέδιο προστασίας. Το προσωπικό αυτό περιλαμβάνει απλούς εργαζόμενους, διευθυντές τμημάτων, προμηθευτές και πελάτες και πιθανόν κάποιες υπηρεσίες, όπως η πυροσβεστική ή η αστυνομία.

2. Ποιες είναι οι κατευθυντήριες γραμμές που θα ακολουθήσει ένα άτομο και ποιος θα είναι ο ακριβής ρόλος του στο σχέδιο προστασίας.

3. Τα μέτρα που πρέπει να ληφθούν για την επαναφορά των κρίσιμων λειτουργιών της επιχείρησης.

Σε όλα τα παραπάνω μπορεί να βοηθήσει η ύπαρξη κάποιων καλά σχεδιασμένων διαδικασιών όπως:

Α) Διαδικασίες για την ανάκτηση απαραίτητων αρχείων και στη συνέχεια για την ενημέρωση τους στην τρέχουσα κατάσταση. Οι περισσότερες εταιρείες φτιάχνουν πολλαπλά αντίγραφα των κρίσιμων δεδομένων, τα οποία αποθηκεύουν σε χώρο, μακριά από το κέντρο επεξεργασίας των δεδομένων.

Β) Διαδικασίες για την επαναλειτουργία του υλικού. Μερικές επιχειρήσεις διαθέτουν ένα δεύτερο εφεδρικό κέντρο δεδομένων, ενώ άλλες, μοιράζονται με άλλες εταιρείες τον ίδιο εξοπλισμό.

Γ) Διαδικασίες για την ανάκτηση του κατάλληλου λογισμικού. Θα πρέπει να υπάρχει διαθέσιμο ένα αντίγραφο του λειτουργικού συστήματος, καθώς επίσης και του λογισμικού εφαρμογών.

Δ) Διαδικασίες για την ανάκτηση λειτουργιών ή τη μεταφορά τους σε κάποιο διαφορετικό σημείο. Είναι πολύ πιθανό, μια πυρκαγιά να μην προκαλέσει καμιά ζημιά στο κέντρο δεδομένων, αλλά στο χώρο εργασίας των χρηστών. Είναι όμως απαραίτητο να συνειδητοποιήσει ο διαχειριστής του συστήματος ότι αν κάποιες λειτουργίες εκτός του κέντρου δεδομένων καταστραφούν, το κόστος επαναφοράς τους μπορεί να είναι αρκετά μεγάλο.

3.4.3. Εναλλακτικές θέσεις κέντρου δεδομένων

Όταν συμβαίνει μία καταστροφή στο Κέντρο Δεδομένων, αυτό θα πρέπει να επανεγκατασταθεί σε μια νέα θέση. Υπάρχουν 4 στρατηγικές:

1) Αμοιβαία συμφωνία με άλλες επιχειρήσεις:δηλαδή η επιχείρηση Α η οποία υπέστη την καταστροφή, έχει προσυμφωνήσει με την επιχείρηση Β να χρησιμοποιεί το κέντρο δεδομένων της, για όσο χρόνο απαιτείται για τη αποκατάσταση των ζημιών. Το κύριο πλεονέκτημα αυτής της στρατηγικής είναι το χαμηλό της κόστος. Αντίθετα, οι δυο επιχειρήσεις θα πρέπει να μειώσουν στο ελάχιστο τις υπηρεσίες επεξεργασίας των δεδομένων ,με αποτέλεσμα και οι δυο να 'αδυνατίσουν'. Ακόμη χειρότερα, η καταστροφή

μπορεί να επιδράσει και τις δυο επιχειρήσεις (π.χ. σεισμός), ώστε καμιά επιχείρηση να μην έχει δυνατότητα επεξεργασίας δεδομένων.

2) Μια δεύτερη στρατηγική αναπλήρωσης του κέντρου δεδομένων είναι η δημιουργία ενός νέου κέντρου δεδομένων από την αρχή. Η επιχείρηση πρέπει να διαθέσει το υλικό (hardware) και να εγκαταστήσει ολόκληρο το υπολογιστικό σύστημα. Αυτή η στρατηγική μειονεκτεί στο σημείο ότι η εκ νέου εγκατάσταση πρέπει να γίνει όσο το δυνατό γρηγορότερα, θέτοντας πιεστικούς χρονικούς περιορισμούς.

3) Μια τρίτη προσέγγιση η οποία εγγυάται τη γρήγορη επαναφορά του κέντρου δεδομένων στην αρχική του κατάσταση είναι η προσέγγιση HOT SITE. Το κέντρο δεδομένων προϋπάρχει για το σκοπό αυτό και μπορεί να το μοιράζονται πολλές επιχειρήσεις. Όταν η καταστροφή είναι γενική ,περιλαμβάνει έναν μεγάλου μεγέθους υπολογιστή (mainframe), ο οποίος είναι συμβατός ή ίδιος με αυτόν που αναπληρώνει. Αυτή η στρατηγική μπορεί να είναι πολύ ακριβή αλλά ελαχιστοποιεί το χρόνο επαναφοράς και επιτρέπει στην επιχείρηση να επαναλειτουργήσει σε μερικές μόνο ώρες.

4) Μια παραλλαγή της στρατηγικής HOT SITE χαμηλότερου όμως κόστους, μπορεί να χρησιμοποιηθεί από εταιρείες που διαθέτουν περισσότερα από ένα κέντρο δεδομένων. Στην περίπτωση μιας καταστροφής, ένα από αυτά τα κέντρα μπορεί να χρησιμοποιηθεί σαν εφεδρικό.

5) Το δεύτερο κέντρο δεδομένων είναι σε θέση να παράσχει υποστήριξη για όλες τις απαραίτητες εφαρμογές της επιχείρησης.

3.4.4. Έλεγχος πυρκαγιάς

Οι πυρκαγιές αποτελούν την πιο πιθανή φυσική απειλή για ένα υπολογιστικό σύστημα. Η καλύτερη αντιμετώπιση για να μην χάνονται τα δεδομένα στην περίπτωση της φωτιάς, είναι να αποθηκεύονται τα δεδομένα και τα προγράμματα σε κάποια άλλη θέση. Επιπλέον, πολλά υπολογιστικά κέντρα χρησιμοποιούν ανιχνευτές φωτιάς και καπνού, οι οποίοι απελευθερώνουν ένα ειδικό αέριο (αφού το νερό είναι απαγορευτικό για τους υπολογιστές). Το κόστος αυτού του αερίου είναι αρκετά υψηλό.

3.5. Λειτουργικά συστήματα Η/Υ

Τα προγράμματα που λειτουργούν σ'ένα Ηλεκτρονικό Υπολογιστή, το λογισμικό ή software όπως ονομάζονται, είναι προγράμματα που ελέγχουν τη

λειτουργία του Η/Υ και αναλαμβάνουν την εκτέλεση μη εξειδικευμένων εργασιών που χρειάζεται σε όλα τα προγράμματα (π.χ. ανάγνωση /εγγραφή πληροφοριών σε όλες τις περιφερειακές συσκευές). Το σύνολο των προγραμμάτων της κατηγορίας αυτής αποτελεί αυτό που ονομάζεται **Λειτουργικό Σύστημα (operating system).**

Το Λειτουργικό Σύστημα παίζει το ρόλο του ενδιάμεσου μεταξύ χρήστη και hardware του υπολογιστή. Σκοπός του είναι να δημιουργήσει ένα περιβάλλον στο οποίο ο χρήστης να μπορεί να εργαστεί. Συχνά το παρομοιάζουν με την κυβέρνηση. Αυτή η ίδια δεν κάνει τίποτα περισσότερο από το να δημιουργεί τις προϋποθέσεις ώστε άλλοι να μπορούν να παράγουν έργο. Κύριες επιδιώξεις ενός Λ. Σ. είναι πρώτον, να κάνει ¨άνετη¨ και ¨φιλική¨ τη χρήση του συστήματος και δεύτερον να εξασφαλίσει την αποδοτική χρήση των μέσων που παρέχει το hardware.

ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ

Θα εστιάσουμε την προσοχή μας στις προϋποθέσεις που απαιτούνται, ώστε ένα Λ. Σ. να διαθέτει τρεις βασικές ιδιότητες που το χαρακτηρίζουν συνολικά ως ¨Ασφαλές¨, δηλαδή :

- Ακεραιότητα (integrity)
- Διαθεσιμότητα (availability)
- Εμπιστευτικότητα (confidentiality)

3.5.1. Ακεραιότητα

Ακεραιότητα ενός Λ.Σ. ονομάζεται η ιδιότητα του συστήματος να προστατεύει τους χρήστες και τα αντικείμενα, υπό οποιαδήποτε, γενικά, συνθήκες. Επίσης να εξασφαλίζει:

• Τη λογική ορθότητα την αξιοπιστία, και την ανοχή σε σφάλματα του υλικού και του λογισμικού του συστήματος,

• Τη λογική πληρότητα των μηχανισμών εξασφάλισης του υλικού και λογισμικού,

• Τη συνοχή των δομών των δεδομένων και την ακρίβεια των αποθηκευμένων δεδομένων.

3.5.2. Διαθεσιμότητα

Διαθεσιμότητα ενός Λ.Σ. είναι η ιδιότητα του να εξασφαλίζει στους εξουσιοδοτημένους χρήστες την πρόσβαση στα αντικείμενα του συστήματος που επιθυμούν ,με τον αποδοτικότερο τρόπο.

Αυτό σημαίνει ότι το σύστημα πρέπει να λειτουργεί ώστε, όχι μόνο να προστατεύει από τους μη εξουσιοδοτημένους χρήστες, αλλά να προστατεύει τα δικαιώματα και των εξουσιοδοτημένων χρηστών. Η διαθεσιμότητα ενός Λ.Σ. είναι συχνά αντιφατική με τις διαδικασίες εξασφάλισης του. Έτσι, αν οι διαδικασίες αυτές εφαρμόζονται συχνά και απαιτούν σημαντικό χρόνο, τότε μειώνεται ο ωφέλιμος χρόνος που διατίθεται στον χρήστη, άρα και η συνολική διαθεσιμότητα του συστήματος.

Η συνύπαρξη των ιδιοτήτων ασφαλείας και διαθεσιμότητας, είναι θέμα ισορροπίας μεταξύ της επιδιωκόμενης φιλικότητας και αξιοπιστίας ενός σχεδιαζόμενου Λ.Σ.

3.5.3. Εμπιστευτικότητα

Εμπιστευτικότητα ενός Λ.Σ. είναι η ιδιότητα του Λ.Σ. να επιτρέπει την πρόσβαση σε αντικείμενα του μόνο σε εξουσιοδοτημένους χρήστες, σύμφωνα με τις αρχές λειτουργίας του.

3.6. Θεμελιώδεις αρχές προστασίες

Υπάρχουν δυο βασικοί στόχοι για την προστασία ενός Λ.Σ., η κατασταλτική προστασία και η προληπτική προστασία.

3.6.1. Κατασταλτική προστασία

Η κατασταλτική προστασία πραγματοποιείται με χρήση μιας σειράς μεθόδων, η βασικότερη από τις οποίες είναι η μέθοδος της επίβλεψης (surveillance). Η μέθοδος αυτή στοχεύει στην καταγραφή κάθε μη εξουσιοδοτημένης απόπειρας στο Λ.Σ. Στοχεύει επίσης στη διαρκή παρακολούθηση της συνολικής λειτουργίας του συστήματος ώστε να εξασφαλίζεται ότι οι μηχανισμοί προστασίας του λειτουργούν κανονικά. Η μέθοδος χρησιμοποιεί δύο τεχνικές:την παρακολούθηση των διαρροών (threat monitoring) και την εποπτεία της ασφάλειας του (security audit).

Η παρακολούθηση των διαρροών σκοπεύει στην άμεση αποκάλυψη κάθε απόπειρας παραβίασης του Λ.Σ. και στη λήψη των απαραίτητων μέτρων για την ακύρωση τους. Η εποπτεία της ασφάλειας αποσκοπεί στην καταγραφή των γεγονότων που σχετίζονται με την ασφάλεια του Λ.Σ. Η καταγραφή αυτή εξασφαλίζει τα απαιτούμενα ιστορικά στοιχεία, ώστε να εντοπιστεί κάποια παραβίαση εκ των υστέρων. Αν και η τεχνική αυτή είναι παθητική, παρόλα αυτά είναι πολύ χρήσιμη γιατί βοηθά στην αποκάλυψη των μεθόδων που χρησιμοποιήθηκαν για την παραβίαση ενός συστήματος.

Η τεχνική αυτή στηρίζεται σε ενέργειες όπως:

- ✓ Παρακολούθηση της λειτουργίας των διαδικασιών ασφαλείας
- ✓ Αναγνώριση των παραβιάσεων και αναφορά τους
- ✓ Διάγνωση της φύσης της παραβίασης κλπ.

3.6.2. Προληπτική προστασία

Η προληπτική προστασία αφορά σε παραβιάσεις που δεν πρόλαβαν να πραγματοποιηθούν και για το λόγο αυτό έχει μεγαλύτερη σπουδαιότητα από την κατασταλτική, αφού το σύστημα δεν έχει υποστεί οποιαδήποτε συνέπεια. Υλοποιείται με βάση δύο αρχές:

- ✓ Την αρχή της ελεγχόμενης προσπέλασης (controlled access)
- ✓ Την αρχή του διαχωρισμού (isolation)

3.6.2.1. Ελεγχόμενη προσπέλαση

Η ελεγχόμενη προσπέλαση επιτυγχάνεται με χρήση τεχνικών που επιτρέπουν σε κάθε εξουσιοδοτημένο χρήστη να αποκτά πρόσβαση μόνο στα αντικείμενα του συστήματος που δικαιούται.

3.6.2.2. Διαχωρισμός

Η αρχή του διαχωρισμού στηρίζεται στη διαδικασία κατά την οποία ένα σύστημα (χρήστες, Λ.Σ. πληροφορίες, φυσικά μέσα) ενός πληροφοριακού συ-

στήματος διαχωρίζεται απολύτως από άλλα συστατικά στα οποία δεν πρέπει να έχει πρόσβαση.

Υπάρχουν αξιόπιστες μέθοδοι οι οποίες πετυχαίνουν το στόχο του διαχωρισμού, σε σημαντικό βαθμό. Χαρακτηριστικά παραδείγματα αποτελούν:

- Η χρήση πυρήνα ασφαλείας (security kernel)
- Η σχεδίαση ιδεατής μνήμης (virtual memory)
- Η σχεδίαση κατανεμημένων συστημάτων (distributed systems).

3.7. Κύριες λειτουργίες λειτουργικών συστημάτων.

Οι λειτουργίες που περιλαμβάνει ένα Λ.Σ. χωρίζονται στις εξής κατηγορίες:

- Λειτουργίες διαχείρισης των μέσων του Η/Υ όπως η κεντρική μονάδα επεξεργασίας, η μνήμη, οι περιφερειακές μονάδες.
- Επικοινωνία με το χειριστή για την εκτέλεση διαφόρων εργασιών ή προγραμμάτων, την ανακοίνωση λαθών ή βλαβών ή την εμφάνιση της τρέχουσας κατάστασης του συστήματος (εργασίες υπό εκτέλεση, κατανομή χώρου του δίσκου).
- Επεξεργασία αρχείων. Περιλαμβάνει τις βασικές εργασίες εισόδου /εξόδου σε μαγνητικά μέσα, την οργάνωση των στοιχείων σε αυτά, υποστήριξη δομών αρχείων και άλλες παρόμοιες εργασίες.
- Εκτυπώσεις στοιχείων σε εκτυπωτές διαφόρων τύπων είτε άμεσα είτε ετεροχρονισμένα
- Επικοινωνία μέσω δικτύου με τοπικούς ή απομακρυσμένους σταθμούς (LAN's data communication).
- Επικοινωνία με προγράμματα εφαρμογών για την εκτέλεση διαφόρων λειτουργιών (system interface).

3.8. Βασικά σημεία ευπάθειας ενός Λ.Σ.

Η ασφάλεια ενός πληροφοριακού συστήματος βασίζεται στις δυνατότητες που παρέχει το Λ.Σ., υπό την εποπτεία του οποίου λειτουργεί. Άρα το λειτουργικό σύστημα αποτελεί τον "ακρογωνιαίο λίθο" της σχεδίασης

και της ασφαλούς λειτουργίας κάθε Π.Σ. Για το λόγο αυτό, αν ένα Λ.Σ. δε διαθέτει τις απαιτούμενες δυνατότητες εξασφάλισης των χρηστών και των αντικειμένων, τότε υπάρχει κίνδυνος να υποστεί κάποια από τις παρακάτω συνέπειες:

- Να υποβαθμιστεί ή και να διακοπεί η λειτουργία του Π.Σ., προσωρινά ή ακόμη και μόνιμα.

- Να επιτραπεί η προσπέλαση κάποιου χρήστη σε διαβαθμισμένα δεδομένα, τα οποία τηρούνται σε προστατευμένη περιοχή.

- Να επιτραπεί η τροποποίηση δεδομένων από χρήστες που δεν έχουν την αντίστοιχη εξουσιοδότηση.

Για να αποφευχθούν οι παραπάνω συνέπειες, πρέπει οι σχεδιαστές ενός Λ.Σ. να γνωρίζουν τα βασικότερα σημεία ευπάθειας του (vulnerabilities). Μερικά από τα πολυάριθμα αυτά σημεία τα οποία αφορούν τα Λ.Σ. είναι:

Δυνατότητα επαναχρησιμοποίησης της μνήμης (scavenging), ελλιπής έλεγχος παραμέτρων (incomplete parameter checking), τροποποιήσεις κώδικα (Trojan horses, computer viruses), ασύγχρονες διακοπές (asynchronous interrupts)

Ασύγχρονες προσβολές (asynchronous attacks).

3.9. Σχεδιαστικοί στόχοι και μέθοδοι προστασίας.

3.9.1. Γενικά στοιχεία.

Στα σύγχρονα υπολογιστικά συστήματα στα οποία υπάρχει η δυνατότητα να κατανέμονται οι πόροι του συστήματος μεταξύ διαφόρων χρηστών, είναι αυξημένη η ανάγκη για εξασφάλιση των δεδομένων και αρχείων ενός χρήστη. Έτσι έννοιες όπως χρονοδρομολόγηση (scheduling), καταμερισμός και παράλληλη χρήση (parallel use), εκτός από τη σειρά σημαντικών προβλημάτων που έλυσαν, δημιούργησαν την ανάγκη εξασφάλισης από ανεπιθύμητες ενέργειες.

Τα συστατικά ενός υπολογιστικού συστήματος που απαιτούν προστασία είναι μεταξύ άλλων τα εξής :

- Αρχεία και ευρετήρια αρχείων

- Εκτελέσιμα προγράμματα

- Συσκευές υλικού

• Δομές δεδομένων όπως ο σωρός

• Μνήμη άμεσης προσπέλασης (RAM)

• Εντολές του λειτουργικού συστήματος οι οποίες καθορίζουν προνόμια στους χρήστες

Δεδομένα του λειτουργικού συστήματος όπως πίνακες διευθύνσεων διακοπών κτλ.

Τα παραπάνω συστατικά του συστήματος μπορούν να αναφέρονται επιγραμματικά ως αντικείμενα του συστήματος.

3.10. Σχεδιαστικοί στόχοι ενός Λ.Σ και μέθοδοι υλοποίησης.

Για να είναι δυνατή η προστασία των αντικειμένων αυτών, πρέπει να έχει προηγηθεί κατάλληλη σχεδίαση του Λ. Σ. Οι στόχοι-μέθοδοι, στους οποίους η σχεδίαση αυτή πρέπει να αποβλέπει είναι οι εξής :

Φυσικός διαχωρισμός (Physical Separation) διαδικασιών. Με τη μέθοδο αυτή κάθε χρήστης διαθέτει συσκευές και χώρο μνήμης τον οποίο χρησιμοποιεί αποκλειστικά ο ίδιος.

Προσωρινός διαχωρισμός (*Temporary Separation) διαδικασιών. Με τη μέθοδο αυτή οι διαδικασίες διαφορετικής διαβάθμισης εκτελούνται σε διαφορετικά χρονικά διαστήματα.*

Λογικός διαχωρισμός (Logical Separation) *ή απομόνωση. Με τη μέθοδο αυτή οι χρήστες μπορούν να εργάζονται διαδοχικά, χρησιμοποιώντας τα ίδια μέσα του συστήματος, αλλά δεν είναι δυνατή καμία ανταλλαγή δεδομένων μεταξύ τους.*

Κρυπτογραφικός διαχωρισμός (Cryptographic Separation). Με τη μέθοδο αυτή είναι δυνατόν δυο χρήστες να μοιράζονται τα ίδια μέσα του συστήματος, σε διαδοχική βάση, έχοντας δικαίωμα προσπέλασης ο ένας στα δεδομένα το υ άλλου.

Η βασική διαφορά από την προηγούμενη μέθοδο είναι ότι τα δεδομένα είναι κρυπτογραφημένα, ώστε μόνο ο νόμιμος κάτοχος τους ή όσοι εξουσιοδοτούνται από αυτόν μπορούν να τα αναγνωρίζουν. Από τις προαναφερθείσες μεθόδους η ασφαλέστερη φαίνεται ότι είναι η μέθοδος του *Φυσικού διαχωρισμού*. Όμως Φυσικός διαχωρισμός υποβαθμίζει σοβαρά την αποδοτικότητα ενός συστήματος, ιδιαίτερα στο βαθμό που η ανταλλαγή δεδομένων είναι από τους βασικότερους στόχους ενός υπολογιστικού συστήματος. Αντίθετα ο κρυπτογραφικός διαχωρισμός, αν και είναι σχετικά ευπαθής μέθοδος, διευκολύνει την ανταλλαγή δεδομένων και πόρων του

συστήματος. Ο απαιτούμενος διαχωρισμός αφορά κάποια διαδικασία ενός χρήστη και μπορεί να έχει μεταβλητό επίπεδο αποτελεσματικότητας. Έτσι τα Λ.Σ. πρέπει να είναι σχεδιασμένα κατά τέτοιο τρόπο ώστε να παρέχουν μεθόδους που εξασφαλίζουν κάποια από τα εξής επίπεδα προστασίας:

• Καμία προστασία. Το επίπεδο αυτό παρέχεται σε διαδικασίες που δεν απαιτούν καμία εξασφάλιση

• Απομόνωση (ISOLATION). Το επίπεδο αυτό παρέχεται από Λ.Σ. που εξασφαλίζουν την δυνατότητα σε δυο διαδικασίες να εκτελούνται διαδοχικά, χωρίς σημεία να γνωρίζει την παρουσία της άλλης.

• Κοινή ή αποκλειστική χρήση (SHARE ALL OR SHARE NOTHING). Η προστασία αυτή παρέχεται από το Λ.Σ. που χαρακτηρίζουν κάθε αντικείμενο του συστήματος κοινό ή ιδιωτικό.

• Δυνατότητες προσπέλασης (SHARE BY CAPABILITIES). Με τη μέθοδο αυτή κάθε χρήστης έχει την δυνατότητα της δυναμικής μεταβολής των δικαιωμάτων που διαθέτει ο ίδιος ή άλλος χρήστης σε αντικείμενα του συστήματος.

• Περιορισμένη χρήση (LIMITED USE) ενός αντικειμένου. Με τη μέθοδο αυτή δεν ελέγχεται μόνο το δικαίωμα προσπέλασης ενός χρήστη σε ένα αντικείμενο, αλλά και τα δικαιώματα των ενεργειών του στο αντικείμενο αυτό.

• Περιορισμοί προσπέλασης (SHARE LIMITATION). Με τη μέθοδο αυτή κάθε χρήστης έχει ή δεν έχει δικαίωμα προσπέλασης σε κάθε αντικείμενο του συστήματος. Τα δικαιώματα καθορίζονται με την χρήση καταστάσεων ή πινάκων που βρίσκονται στη διάθεση του Λ.Σ.

Από όλα τα παραπάνω προκύπτει ότι η σχεδίαση ενός Λ.Σ. με αυξημένες δυνατότητες εξασφάλισης των αντικειμένων του δεν είναι αυτοσκοπός. Θα πρέπει να συνεκτιμηθεί το γενικότερο λειτουργικό περιβάλλον στο οποίο απευθύνεται το σύστημα, η επένδυση που απαιτείται για την ανάπτυξη του, καθώς και η γενικότερη εξέλιξη στο τομέα της ασφάλειας των πληροφοριακών συστημάτων.

3.11. Πρότυπα σχεδίασης ασφαλών Λ. Σ.

Προϋποθέσεις σχεδίασης ασφαλών Λ. Σ. Για τη σχεδίαση ενός ασφαλούς Λ.Σ. απαιτείται η ικανοποίηση των παρακάτω προϋποθέσεων:

• Πολιτική Εξασφάλισης (SECURITY POLICY). Πρέπει να υπάρχει μια σαφής δέσμη βασικών αρχών, η οποία να περιλαμβάνει τους στόχους των σχεδιαστών του Λ.Σ.

• Ταυτοποίηση (IDENTIFICATION). Κάθε αντικείμενο του συστήματος πρέπει να μπορεί να αναγνωρισθεί θετικά.

• Σήμανση (MARKING). Κάθε αντικείμενο του συστήματος πρέπει να συνοδεύεται από μια ένδειξη του βαθμού εμπιστευτικότητάς του.

• Ελεγκτότητα (ACCOUNTABILITY). Το Λ. Σ. πρέπει να καταγράφει όλες τις ενέργειες που αφορούν ή μπορούν να επηρεάσουν την ασφάλειά του.

• Διαβεβαίωση (ASSURANCE). Το σύστημα πρέπει να παρέχει τεχνικές ρυθμίσεις για την υλοποίηση της πολιτικής εξασφάλισής του, οι οποίες μπορούν να εκτιμηθούν ως προς την αποτελεσματικότητά τους.

• Συνεχής προστασία (CONTINUOUS PROTECTION). Οι τεχνικές εξασφάλισης του Λ. Σ. πρέπει να προστατεύονται από κάθε ανεπιθύμητη μετατροπή.

3.12. ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ.

Η ασφάλεια των συστημάτων Β.Δ. (Βάσεων Δεδομένων) παίζει πολύ σημαντικό ρόλο στη γενικότερη ασφάλεια των πληροφοριακών συστημάτων. Δύο βασικοί λόγοι γι'αυτό είναι αφενός μεν η φύση και ο ρόλος αυτής της τεχνολογίας (Διαχειρίζεται και μεταδίδει συλλογές από συνήθως μερικά ή ολικά δεδομένα), και αφετέρου η ευρύτατη διάδοση της τα τελευταία χρόνια (Υπολογίζεται ότι το 90% των συστημάτων υπολογιστών που πωλούνται σήμερα διαθέτουν κάποιας μορφής σύστημα Β.Δ. Πέρα από τις συνηθισμένες παραμέτρους τις σχετικές με την ασφάλεια των πληροφοριακών συστημάτων όπως η ακεραιότητα (integrity), έλεγχος προσπέλασης (access control), έλεγχος (auded), κλπ τα Σ.Β.Δ. εισάγουν και νέους, όπως διακριτότητα (granoularity), έμμεση προσπέλαση (inference) aggrecation , filtering, journaling, κ.λ.π. Τα Σ.Β.Δ προσφέρουν ακόμη νέα εργαλεία για την εφαρμογή και τον έλεγχο της ασφάλειας του Π.Σ. Κάνουν επίσης εφικτή την εύκολη εφαρμογή συγκεκριμένων πολιτικών ασφάλειας, όχι μόνο σε επίπεδο εγγραφής (record level), αλλά ακόμα και σε επίπεδο επιμέρους δεδομένων της βάσης (data item level). Το επίπεδο και οι προδιαγραφές ασφάλειας ενός τύπου δεδομένων της βάσης μπορεί έτσι να είναι εύκολα διαφορετικά από αυτά ενός άλλου τύπου δεδομένων της ίδιας εγγραφής. Με άλλα λόγια το επίπεδο και οι προδιαγραφές ασφάλειας ενός στοιχείου, (δεδομένο), μιας σχετικής Β.Δ. μπορεί να είναι διαφορετικά από αυτά των άλλων στοιχείων της ίδιας γραμμής ή στήλης της ίδιας σχέσης (πίνακας).

Θα πρέπει να παρατηρήσουμε πάντως ότι, παρά την ιδιαίτερη σημασία της, η μέχρι σήμερα έρευνα σχετικά με τη ασφάλεια συστημάτων Β.Δ είναι πολύ περιορισμένη σε σχέση με τις άλλες τρεις βασικές συνιστώσες του προβλήματος. Ένας βασικός λόγος γι'αυτό είναι το γεγονός ότι πρόκειται για μια σχετικά πρόσφατη τεχνολογία, που μάλιστα μόλις τα τελευταία χρόνια έφτασε στο στάδιο της γενικής εφαρμογής και αποδοχής. Ένας άλλος λόγος είναι ότι μέχρι και πρόσφατα το πρόβλημα της ασφάλειας των Σ.Β.Δ. θεωρείτο

ένα μερικό πρόβλημα αυτού της γενικότερης ασφάλειας του υπολογιστικού συστήματος (OPERATING SYSTEM SECURITY), κάτι που όπως θα δούμε στη συνέχεια δεν είναι ακριβές σήμερα.

3.12.1. Ορισμός-γενικό πλαίσιο.

Αντικείμενο της θεωρίας της ασφάλειας των Σ.Β.Δ. είναι όπως προαναφέρθηκε η μελέτη της ικανότητας του συστήματος να εφαρμόσει μια προκαθορισμένη πολιτική προστασίας των πληροφοριών (SECURITY POLICY) που περιλαμβάνονται στη Β.Δ. Αφορά δε τη δυνατότητα προσπέλασης, την διαθεσιμότητα και την δυνατότητα τροποποίησης ή διαγραφής των πληροφοριών της βάσης. Οι χρήστες ενός Π.Σ. χρησιμοποιούν συνήθως τη Β.Δ. σαν ένα τεχνικό εργαλείο για την αποθήκευση, επεξεργασία και μετάδοση πληροφοριών. Η Β.Δ. μεταδίδει τις πληροφορίες ακολουθώντας την παρακάτω βασική διαδικασία:

"Υποβολή Ερωτήσεων (ACCEPT MESSAGES) ⟶

Αποθήκευση/Επεξεργασία Δεδομένων ⟶

/Αναπαραγωγή/Μετάδοση δεδομένων όταν ζητηθούν".

Η αξιοπιστία της μετάδοσης ελέγχεται από ειδικά πρωτόκολλα που εγγυώνται την ολοκλήρωση των παραστατικών (transaction) και την εφαρμογή των κανόνων ακεραιότητας (integrity constraints) στα δεδομένα της βάσης.

Οι παρακάτω γενικές αρχές που σχετίζονται με την ασφάλεια των Β.Δ. είναι γενικά αποδεκτές σήμερα.

I. Η μελέτη του προβλήματος της ασφάλειας μιας Β.Δ. πρέπει να λαβαίνει υπ'όψιν της το σύνολο του λογισμικού (S/W) και ολικού (H/W) του συστήματος που σχετίζεται άμεσα ή έμμεσα με τις πληροφορίες που κρατιούνται στη Β.Δ. Για παράδειγμα ένα ευάλωτο λειτουργικό σύστημα μπορεί να αχρηστέψει όλα τα μέτρα ασφάλειας που προσφέρει ένα ασφαλές σύστημα διαχείρισης της βάσης δεδομένων.

II. Η ακεραιότητα των δεδομένων είναι βασική απαίτηση και προϋπόθεση. Η βάση δεδομένων πρέπει να διατηρεί σε κάθε περίπτωση την ακεραιότητα των δεδομένων που φυλάσσονται σε αυτήν. Ο χρήστης πρέπει να εμπιστεύεται το σύστημα ότι θα του επιστρέφει τα ίδια δεδομένα που καταχωρήθηκαν σε αυτό, και ότι οποιαδήποτε μεταβολή στα δεδομένα έχει γίνει από εξουσιοδοτημένους και μόνο χρήστες. Τα δεδομένα δεν πρέπει να καταστρέφονται ή μεταβάλλονται είτε τυχαία (π.χ. από βλάβη του συστήματος), είτε σκόπιμα (π.χ από μη εξουσιοδοτημένους χρήστες). Σε κάθε

όμως περίπτωση ο χρήστης πρέπει τουλάχιστον να ενημερώνεται για κάθε παραβίαση της ακεραιότητας των δεδομένων του συστήματος που τον αφορά.

III. Τα δεδομένα πρέπει να είναι άμεσα διαθέσιμα όταν ζητούνται από εξουσιοδοτημένους χρήστες. Για το λόγο αυτό θα πρέπει να υπάρχει ειδική πρόνοια για τις περιπτώσεις π.χ. βλάβες ή μη διαθεσιμότητας του συστήματος.

IV. Οι περιοδικοί ή έκτακτοι έλεγχοι ορθότητας (audit) των δεδομένων της βάσης πρέπει να είναι αρκετά αναλυτικοί και πλήρεις ώστε να είναι αποτελεσματικοί, αλλά ταυτόχρονα θα πρέπει να είναι έτσι δομημένοι, ώστε να μην επηρεάζουν σημαντικά την απόδοση του συστήματος.

V. Βασικός αντικειμενικός σκοπός πρέπει να είναι η επαρκής προστασία της εμπιστευτικότητας (secrecy/prevent disclosure) των πληροφοριών της βάσης και ταυτόχρονα η προστασία της ακεραιότητας και η μεγιστοποίηση της διαθεσιμότητας και της απόδοσης του συστήματος. Έννοιες που συχνά είναι συγκρουόμενες (π.χ. αποτελεσματικότερη προστασία της εμπιστευτικότητας συνεπάγεται συνήθως απώλειες στην απόδοση του συστήματος και την διαθεσιμότητα των πληροφοριών, και αντιστρόφως). Γι'αυτό και θα πρέπει να βρίσκεται κάθε φορά η χρυσή τομή (που βασίζεται συνήθως στην ανάλυση των πιθανών κινδύνων (risk analysis) και των απαιτήσεων ασφάλειας του συγκεκριμένου συστήματος).

3.12.2. Απαιτήσεις ασφάλειας των βάσεων δεδομένων

Οι βασικές απαιτήσεις για την ασφάλεια των συστημάτων Β.Δ. δεν διαφέρουν ουσιαστικά από αυτές του υπολοίπου συστήματος. Οι κυριότερες από αυτές είναι:

I. Φυσική ακεραιότητα της βάσης (physical database integrity). Τα δεδομένα της βάσης πρέπει να είναι προστατευμένα από φυσικά προβλήματα (π.χ. πτώση τάση ρεύματος), ούτως ώστε να είναι δυνατή η επανάκτηση των δεδομένων μετά από μια φυσική καταστροφή.

II. Λογική ακεραιότητα της βάσης (logical database integrity). Πρέπει να διατηρείται σε κάθε περίπτωση η λογική ακεραιότητα της βάσης. Η λογική ακεραιότητα εγγυάται την προστασία της λογικής δομής της βάσης. Για παράδειγμα η διατήρηση της λογικής ακεραιότητας της βάσης εγγυάται ότι η μεταβολή της τιμής ενός από τα πεδία της δεν επηρεάζει τις τιμές άλλων πεδίων, παρά μόνο εφόσον κάτι τέτοιο έχει προβλεφθεί.

III. Ακεραιότητα των πεδίων της βάσης (element integrity). Εγγυάται ότι οι τιμές των επιμέρους πεδίων της βάσης είναι ακριβείς (σωστές).

IV. Έλεγχος προσπέλασης (access control). Εγγυάται ότι οι χρήστες της βάσης μπορούν να προσπελάσουν μόνο τα δεδομένα εκείνα για τα οποία έχουν εξουσιοδοτηθεί. Οι διάφοροι τύποι χρηστών μπορεί έτσι να περιοριστούν σε ορισμένους χώρους και τρόπους προσπέλασης, ανάλογα με τις ανάγκες τους (π.χ. Read only).

V. Πιστοποίηση των χρηστών (user authentication). Η διαδικασία πιστοποίησης εγγυάται ότι ο κάθε χρήστης της βάσης αναγνωρίζεται θετικά από τη βάση, πριν του επιτραπεί η προσπέλαση σε αυτήν.

VI. Διαθεσιμότητα (availability). Εγγυάται ότι οι εξουσιοδοτημένοι χρήστες μπορούν γενικά να προσπελάσουν άμεσα τη βάση και τα δεδομένα για τα οποία είναι εξουσιοδοτημένοι.

3.12.3. Σχεδιασμός συστημάτων ασφαλών Β.Δ.

Το πρόβλημα του σχεδιασμού και της υλοποίησης ενός ασφαλούς συστήματος βάσης δεδομένων μπορεί να αναλυθεί σε τρεις επί μέρους συνιστώσες:

1) Τον καθορισμό των *semantics* ('σημαντικής') της ασφαλούς βάσης που πρόκειται να αναπτυχθεί. Τον προσδιορισμό δηλαδή των ιδιοτήτων ασφάλειας που απαιτούνται με τη βοήθεια των *semantics* της βάσης.

2) Την υλοποίηση των *semantics* αυτών σε ένα σύστημα βάσης δεδομένων, δηλαδή σε ένα Σ.Δ.Β.Δ. και στα δεδομένα που αυτό διαχειρίζεται.

3) Την πιστοποίηση (assurance) ότι το σύστημα που υλοποιήθηκε προσφέρει τις επιθυμητές ιδιότητες ασφάλειας.

Μια μεθοδολογία σχεδιασμού πρέπει να προσδιορίζει αναλυτικά το πως θα υλοποιηθεί κάθε μια από τις παραπάνω τρεις συνιστώσες ανάπτυξης ενός ασφαλούς συστήματος Β.Δ. Αυτό επιτυγχάνεται συνήθως με τη βοήθεια μοντέλων και εργαλείων ανάλυσης και με τη δημιουργία ενός ενιαίου πλαισίου που επιτρέπει την εξασφάλιση συνέπειας (consistency) σε όλη τη διάρκεια της διαδικασίας. Ακόμη, μια τέτοια διαδικασία θα πρέπει να αποτελείται από επιμέρους βήματα (multiphase), ώστε να επιτρέπει τον προοδευτικό προσδιορισμό και υλοποίηση του συστήματος.

Τα επί μέρους βήματα μιας τέτοιας μεθοδολογίας σχεδιασμού και υλοποίησης ενός ασφαλούς συστήματος βάσης δεδομένων περιγράφονται στη συνέχεια. Τα βήματα αυτά είναι αντίστοιχα με εκείνα του γενικού σχεδιασμού ενός συστήματος βάσης δεδομένων. Αυτό δε γιατί ο σχεδιασμός για την ασφάλεια της βάσης (database security design)πρέπει να αντιμετωπίζεται σαν μέρος του γενικού σχεδιασμού της βάσης δεδομένων(overall database

design). Είναι σήμερα γενικά παραδεκτό ότι ο σχεδιασμός για την ασφάλεια της βάσης πρέπει να γίνεται παράλληλα, και όχι να ακολουθεί, όπως συμβαίνει συνήθως, τον γενικό σχεδιασμό.

3.12.3.1. Προκαταρκτική ανάλυση.

Βασικός στόχος της προκαταρκτικής ανάλυσης είναι ο προσδιορισμός των στόχων (scope) των σχετικών με την ασφάλεια της βάσης και της εφικτότητας (feasibility) υλοποίησης τους στο σύστημα υπό σχεδιασμό. Κατά φάση αυτή εξετάζονται:

1) Οι κίνδυνοι (threats) που αντιμετωπίζει το σύστημα στο συγκεκριμένο περιβάλλον λειτουργίας (π.χ. μη εξουσιοδοτημένη προσπέλαση στα δεδομένα, ιοί κλπ).

2) Τα χαρακτηριστικά του περιβάλλοντος (π.χ. το διαθέσιμο ήδη software and hardware, η φυσική ασφάλεια του συστήματος, κ.λ π.).

3) Η καταλληλότητα των προϊόντων software and hardware που είναι εμπορικά διαθέσιμα. Εξετάζεται επίσης το κατά πόσο θα γίνει η ανάπτυξη του ασφαλούς συστήματος εσωτερικά ή από τρίτους.

4) Η συμβατότητα των υφιστάμενων προϊόντων ασφάλειας με το διαθέσιμο εμπορικά software and hardware.

5) Η αναμενόμενη απόδοση του συστήματος σε σχέση με τους αναμενόμενους περιορισμούς.

6) Ο κατάλογος των απαιτήσεων και πολιτικών ασφάλειας. Με τον τρόπο αυτό προσδιορίζονται ανεπίσημα (informally) οι απαιτήσεις και προδιαγραφές ασφάλειας του συστήματος.

7) Η σχέση κόστους και απόδοσης του νέου συστήματος σε σχέση με το επιθυμητό επίπεδο ασφάλειας.

Πρέπει να σημειωθεί ότι οι απαιτήσεις ασφάλειας που προσδιορίζονται κατά την διάρκεια αυτής της φάσης επηρεάζουν σημαντικά την δομή της υπό ανάπτυξη βάση δεδομένων. Σε περιπτώσεις δε υφισταμένων συστημάτων μπορεί να οδηγήσουν σε σημαντικό επανασχεδιασμό του λογικού και φυσικού μοντέλου βάσης.

3.12.3.2. Ανάλυση των απαιτήσεων ασφαλείας.

Κατά την φάση της ανάλυσης των απαιτήσεων (requirements analysis) προσδιορίζεται λεπτομερώς από τον σχεδιαστή το ποίοι είναι οι χρήστες της βάσης και ποιες είναι οι ανάγκες τους. Συνήθως αυτό περιλαμβάνει και τον προσδιορισμό των κατηγοριών πληροφοριών που είναι απαραίτητες για τον κάθε τύπο χρήστη, τα χαρακτηριστικά των πληροφοριών αυτών, και το πως οι συγκεκριμένες αυτές πληροφορίες σχετίζονται με τις υπόλοιπες. Οι πληροφορίες που συγκεντρώνονται σε αυτή τη φάση θα πρέπει να επεκταθούν για να περιλαμβάνουν στην περίπτωση που υλοποιείται για παράδειγμα μια πολιτική ασφάλειας πολλαπλών επιπέδων και τα ακόλουθα:

- Το επίπεδο εξουσιοδότησης για κάθε τύπο χρήστη.
- Τη βασική ηλεκτρονική διεύθυνση κάθε χρήστη.
- Τη συχνότητα, τον όγκο, το βαθμό εμπιστευτικότητας και τη σπουδαιότητα των παραστατικών κάθε τύπου χρήστη
- Λεπτομέρειες για τις απαιτήσεις προσπέλασης κάθε βασικού τύπου παραστατικού
- Ο βαθμός ευαισθησίας (sensitivity level/range) κάθε τύπου δεδομένων
- Τους τρόπους μεταβολής του βαθμού ευαισθησίας κάθε τύπου δεδομένων της βάσης
- Άλλους περιορισμούς ασφάλειας ή διανομής.

Οι πρόσθετες αυτές πληροφορίες είναι απαραίτητες για να προσδιοριστούν οι αντίστοιχες ενδείξεις ευαισθησίας (sensitivity labels) στα δεδομένα της βάσης, να δοθούν οι κατάλληλοι βαθμοί εξουσιοδότησης στους χρήστες και να γίνει ο φυσικός σχεδιασμός της κατανεμημένης βάσης δεδομένων.

3.13. Η ασφάλεια των συστημάτων βάσεων δεδομένων σε σχέση με αυτή των λειτουργικών συστημάτων.

Η ασφάλεια των συστημάτων βάσεων δεδομένων θεωρείται συχνά σαν θυγατρική της ασφάλειας των λειτουργικών συστημάτων και αυτό γιατί σε πολλές περιπτώσεις ένα ασφαλές σύστημα Β.Δ προϋποθέτει ένα ασφαλές Λ.Σ. Συχνά υποστηρίζεται ότι εάν το Λ.Σ. δεν είναι ασφαλές, είναι μάταιο να σχεδιάζεται ένα ασφαλές σύστημα Β.Δ. Η άποψη αυτή δεν είναι σήμερα ακριβής. Αναμφισβήτητα, η ύπαρξη ενός ασφαλούς Λ.Σ. είναι επιθυμητή.

Υπάρχουν όμως πολλές περιπτώσεις (ουσιαστικά η συντριπτική πλειοψηφία) όπου δεν είναι πρακτικά εφικτή η ύπαρξη ενός ασφαλούς Λ.Σ. (είτε λόγω τεχνικών προβλημάτων, είτε λόγω κόστους είτε λόγω προβλημάτων απόδοσης (performance). Για αυτό το λόγο είναι ιδιαίτερα σημαντικό να αναπτυχθούν μέθοδοι που θα διασφαλίζουν το επιθυμητό επίπεδο ασφάλειας της Β.Δ ,ακόμα και στις περιπτώσεις που χρησιμοποιείται ένα κοινό Λ.Σ.

Η ασφάλεια των συστημάτων Β.Δ πιστεύουμε ότι μπορεί σήμερα να είναι σε ένα μεγάλο βαθμό ανεξάρτητη από την ύπαρξη ενός ασφαλούς Λ.Σ. Αυτό μπορεί να επιτευχθεί εάν η προσπέλαση στα δεδομένα της βάσης ελέγχεται για παράδειγμα με κρυπτογραφικές μεθόδους. Αυτό κάνει πολύ δυσκολότερη για παράδειγμα την παράκαμψη του συστήματος διαχείρισης της βάσης δεδομένων κατά την προσπέλαση στα δεδομένα της βάσης.

3.14. Πολιτικές και μέτρα ασφαλείας και προστασίας του απορρήτου.

Ένας σημαντικός παράγοντας της λειτουργίας των Π.Σ. είναι η ασφάλεια του συστήματος και των στοιχείων, ιδιαίτερα στην περίπτωση των νοσοκομείων. Αυτό έχει μια πολύ σοβαρότερη θεώρηση λόγω του ιατρικού απορρήτου. Το σύστημα καθορισμού δικαιωμάτων για την διασφάλιση του απορρήτου και της ασφάλειας ορίζεται σε τέσσερα (4) επίπεδα:

1. Ρόλοι και υπορόλοι: Αρχικά ορίζονται οι ρόλοι, οι οποίοι ουσιαστικά εκφράζουν μια γενική κατηγοριοποίηση των χρηστών. Π.χ. ιατρικό προσωπικό, νοσηλευτικό προσωπικό, διοικητικό προσωπικό κ.λ.π.

2. Υπορόλοι ανά ρόλο: Για κάθε ρόλο ορίζονται αναλυτικότερα οι υπορόλοι, δηλαδή υποκατηγορίες που περιλαμβάνει. Π.χ. θεράπων ιατρός, ιατρός χειρούργος, ειδικευόμενος ιατρός, διευθυντής κλινικής κ.λ.π.

3. Διαδικασίες ανά υπορόλο σε επίπεδο εφαρμογής: Για κάθε υπορόλο και για κάθε κύρια εφαρμογή. Π. χ. τα δικαιώματα επί των δεδομένων, που παρέχονται στον συγκεκριμένο υπορόλο. Τα δικαιώματα αυτά είναι: εμφάνιση, εισαγωγή, διόρθωση, διαγραφή. Για τα ιατρικά δεδομένα όμως, δεν επιτρέπεται σε επίπεδο χρήστη η διαγραφή. Αυτό θα μπορεί να γίνεται σε χαμηλό επίπεδο(supervisor συστήματος) και μόνο μετά από γραπτή απόφαση ανώτερων διοικητικών οργάνων.

4. Κατάταξη χρηστών: Σε κάθε χρήστη αποδίδεται ένας ρόλος και υπορόλος από τον Υπεύθυνο Διαχείρισης σύμφωνα με την προεγκριθείσα από την Διοίκηση κατάταξη. Εξ΄ορισμού ο χρήστης δεν έχει πρόσβαση στις εφαρμογές, ούτε στις διεργασίες της, καθώς και δικαιώματα στα δεδομένα. Η εξουσιοδότηση αυτή αποκτάται με την ανάθεση ρόλου και υπορόλου. Έτσι, ο χρήστης κληρονομεί τα δικαιώματα που έχουν προκαθοριστεί στον υπορόλο του.

Οι εφαρμογές του Ιατρικού Υποσυστήματος έχουν ένα προς ένα αντιστοιχία με τις κλινικές. Έτσι, τα δεδομένα για κάθε χρήστη είναι αυτά που αφορούν τη κλινική του. Αν υπάρχουν περιπτώσεις που απαιτείται η προσπέλαση σε ασθενείς από άλλες κλινικές, τότε μπορεί κάποιος γιατρός να αποκτήσει ένα επιπρόσθετο ρόλο ή υπορόλο. Συνεπώς, ένας χρήστης μπορεί να έχει περισσότερους από έναν ρόλο ή υπορόλο.

ΡΟΛΟΙ

- Μηχανικός Συστήματος
- Προσωπικού Ακτινολογικού
- Διοικητικό Προσωπικό
- Εργαστηριακό Προσωπικό
- **Ιατρικό Προσωπικό**
- Διοίκηση Νοσοκομείου
- Νοσηλευτικό Προσωπικό
- Φαρμακοποιός

ΥΠΟΡΟΛΟΙ ΙΑΤΡΙΚΟΥ ΠΡΟΣΩΠΙΚΟΥ

- **Διευθυντής Κλινικής**
- Ιατρός Χειρούργος
- Διαιτολόγος Ιατρός
- Ιατρός Αναισθησιολόγος
- Ιατρός Επιδημιολογικών Λοιμώξεων
- Ιατρός Έκτακτων Εξωτερικών Ιατρείων
- Ιατρός Τακτικών Εξωτερικών Ιατρείων
- Εργαστηριακός Ιατρός
- Ειδικευόμενος Ιατρός
- Γενικός Εφημερεύων Ιατρός

ΚΑΤΗΓΟΡΙΕΣ

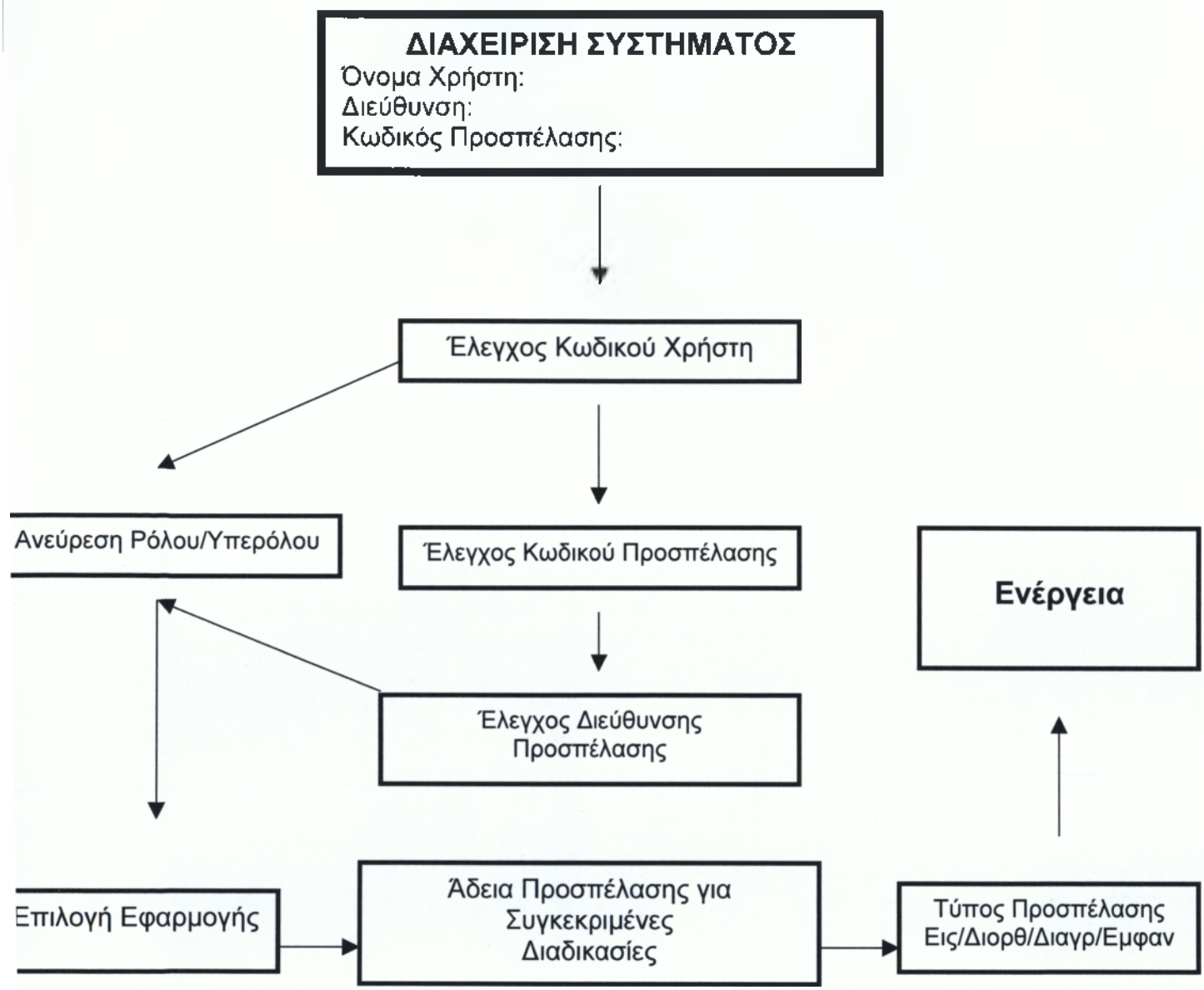
ΕΙΔΙΚΟΤΗΤΕΣ ΙΔΙΟΤΗΤΕΣ

ΕΦΑΡΜΟΓΗ: ΙΑΤΡΙΚΗ ΦΡΟΝΤΙΔΑ ΔΙΑΔΙΚΑΣΙΕΣ ΤΟΥ ΥΠΕΡΟΛΟΥ:ΔΙΕΥΘΥΝΤΗΣ ΚΛΙΝΙΚΗΣ				
ΠΕΡΙΓΡΑΦΗ ΔΙΑΔΙΚΑΣΙΑΣ	ΕΜΦΑΝ	ΕΙΣΑΓ	ΔΙΟΡΘ	ΔΙΑΓΡ
Παραλαβή Χειρογράφου Ιατρικού Φακέλου	X	X	o	o
Έκβαση Προβλήματος Ασθενή	X	X	X	o
Παρακολούθηση Εξετάσεων/Ζωτικών Σημειώσεων	X	X	X	o
Ενεργά Προβλήματα	X	X	X	o
Πορεία Νόσου	X	X	X	o
Σημεία Ασθενή	X	X	X	o
Λήψη Δείγματος	X	X	X	o
Συμπτώματα Ασθενή	X	X	X	X
Μετάγγιση Αίματος	X	X	X	X

Η πολιτική αυτή θα πρέπει να εγκριθεί από τη Διοίκηση και θα πρέπει να ληφθούν υπ' όψη όλες οι νομοθετικές και λειτουργικές παράμετροι οι οποίες θα εξασφαλίζουν την ασφάλεια και το απόρρητο, χωρίς να δημιουργούν λειτουργικά προβλήματα εκεί που δε χρειάζεται.

Εκτός της πολιτικής που αναπτύχθηκε και δημιουργείται μέσω της εφαρμογής, μια άλλη κατηγορία ασφαλείας ορίζεται στο επίπεδο του λειτουργικού συστήματος UNIX. Ο ορισμός του γίνεται μέσω του Κωδικού Χρήστη (password).

Απαιτούνται διαδικασίες διαφύλαξης του απορρήτου, οι οποίες αφορούν κυρίως την επαφή άλλου προσωπικού, εκτός του ιατρικού με τα στοιχεία αυτά (τεχνικοί, σύμβουλοι, προμηθεύτρια εταιρεία). Στις περιπτώσεις αυτές θα πρέπει να γίνονται ειδικά δεσμευτικά συμφωνητικά μεταξύ του νοσοκομείου και όσων τυχόν έρχονται σε επαφή με το σύστημα και τα στοιχεία που έχουν ευαισθησία.


ΔΙΑΧΕΙΡΙΣΗ ΣΥΣΤΗΜΑΤΟΣ
Όνομα Χρήστη:
Διεύθυνση:
Κωδικός Προσπέλασης:
Έλεγχος Κωδικού Χρήστη
Ανεύρεση Ρόλου/Υπερόλου
Έλεγχος Κωδικού Προσπέλασης
Ενέργεια
Έλεγχος Διεύθυνσης Προσπέλασης
Επιλογή Εφαρμογής
Άδεια Προσπέλασης για Συγκεκριμένες Διαδικασίες
Τύπος Προσπέλασης Εις/Διορθ/Διαγρ/Εμφαν

3.15. Πολιτικές και μέτρα υλοποίησης

Περιλαμβάνει ενέργειες και διαδικασίες που αφορούν τη διοίκηση του έργου, τους χρήστες, τα δεδομένα, προτεραιότητες, φάσεις εγκατάστασης και πιλοτικά σχέδια.

3.15.1. Οργανωτική διοίκηση του έργου

Η οργανωτική δομή της διοίκησης του έργου αναλύεται σε τρία επίπεδα από την πλευρά του νοσοκομείου, όπως παρουσιάζεται στο επόμενο οργανωτικό σχήμα. Στο πάνω επίπεδο βρίσκεται η Εφορεία του νοσοκομείου, η οποία ελέγχει και εγκρίνει την διάθεση των πόρων, τις πολιτικές απόκτησης και επέκτασης των συστημάτων και τις πολιτικές ελέγχου και διαδικασιών που απαιτούνται για την αποδοχή και λειτουργία του Π.Σ.

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ

Κρίσιμα Σημεία-Διαδικασίες σε ένα Νοσοκομειακό Πληρο-φοριακό Σύστημα.

Περίληψη 4ου κεφαλαίου.

Στην εργασία αυτή ορίζεται η *Ασφάλεια* και τονίζεται η σημασία της για τα *Νοσοκομειακά Πληροφοριακά Συστήματα* και τη λειτουργία των νοσοκομείων γενικότερα. Γίνεται αναφορά στη σημασία των *εναλλακτικών κέντρων πληροφορικής* και στην *αναγκαιότητα ύπαρξης ενός πλήρους σχεδίου έκτακτης ανάγκης*. Ακολούθως, εξετάζονται αναλυτικά και δίνεται έμφαση στους κινδύνους αλλά και στα μέτρα που πρέπει να ληφθούν για να καλυφθούν επαρκώς:

1. **Η Φυσική Ασφάλεια των πληροφοριακών συστημάτων**
2. **Η Λογική Ασφάλεια των πληροφοριακών συστημάτων**
3. **Η Ασφάλεια των λοιπών Δικτύων του περιφερειακού και βοηθητικού εξοπλισμού.**

Στη συνέχεια αναπτύσσονται οι *«περιοχές»* ελέγχου του κέντρου πληροφορικής, ενώ παράλληλα γίνεται αναφορά στις διάφορες τεχνικές ελέγχου.

4. Κρίσιμα Σημεία-Διαδικασίες σε ένα Νοσοκομειακό Πληροφοριακό Σύστημα.

ΕΙΣΑΓΩΓΗ: Ασφάλεια Νοσοκομειακών Πληροφοριακών Συστημάτων είναι η ικανότητα του οργανισμού να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες κάθε στιγμή αναζήτησης.

Η προαναφερόμενη ικανότητα του νοσοκομείου στηρίζεται στη λήψη μέτρων τα οποία εξασφαλίζουν:

1. Την ακεραιότητα των δεδομένων.
2. Την εμπιστευτικότητα των δεδομένων.
3. Την αδιάλειπτει λειτουργία του κέντρου πληροφορικής.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι ικανή σε συνεργασία με τις άλλες βασικές προϋποθέσεις λειτουργίας ενος οργανισμού στην εξασφάλιση της εύρυθμης λειτουργίας του.

Η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του νοσοκομείου. Θα πρέπει δε,να αποδεκτούμε το κόστος της ασφάλειας και σαν κόστος χρόνου και σαν κόστος χρήματος. Το κόστος για την ασφάλεια των Πληροφοριακών συστημάτων προκύπτει απο την εκάστοτε «πολιτική» που ακολουθεί ο οργανισμός. Η πολιτική αυτή καθορίζεται απο μια δυναμική εκτίμηση των μέτρων ασφαλείας σε σχέση με τις συνέπειες που θα έχει για το Νοσοκομείο οποιαδήποτε δυσλειτουργία. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, και για κάθε θέμα που απαιτείται κάποιο μέτρο ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί ενα γεγονός σε σχέση με τις συνέπειες που δημιουργεί. Εάν η τιμή και των δυο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να λήφθουν μέτρα, ανεξάρτητα απο το κόστος. Απαιτείται συνεπώς πολιτική ασφάλειας η οποία θα πρέπει να εξισορροπεί το κόστος ασφαλείας απο την μια πλευρά και το κόστος απο πιθανολογούμενο κίνδυνο απο την άλλη. Επίσης θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μην παρεμποδίζεται η ευελιξία και η ανάπτυξη του οργανισμού.

Τέλος, η ασφάλεια είναι απο τη φύση της δυναμική παράμετρος και όχι στατική, διότι η τεχνολογία και η συνεχώς βελτιούμενη επιτηδειότητα των απατεώνων απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς και η πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

4.1. Ασφάλεια νοσοκομειακών πληροφοριακών συστημάτων –προστασία (ΠΡΟΛΗΨΗ και ΘΕΡΑΠΕΙΑ).

Σε πολύ γενικές γραμμές η ασφάλεια των Ν.Π.Σ. διακρίνεται σε:

I. Ασφάλεια στην περίπτωση έκτακτης ανάγκης.

II. Ασφάλεια στις καθημερινές διεργασίες.

4.1.1. Ασφάλεια στην περίπτωση έκτακτης ανάγκης.

Οι συνθήκες περίπτωσεις δυσλειτουργίας ενός κέντρου πληροφορικής απο διακοπές ηλεκτρικής ενέργειας, προσωρινές βλάβες απο πλυμμήρα ή πυρκαϊά,΄΄πτώση΄΄μέρους του εξοπλισμού και του κεντικού Η/Υ, αντιμετωπίζεται συνήθως με μετάπτωση στο εφεδρικό σύστημα που υπάρχει συνήθως στα νοσοκομεία ή προκαλείται κάποια καθυστέρηση στην λειτουργεία των διαδικασιών του οργανισμού μέχρι την αποκατάσταση των βλαβών και την πλήρη λειτουργία του εξοπλισμού. Με τον όρο έκτακτη ανάγκη εννοείται τέτοιας έκτασης καταστροφή στο κέντρο πληροφορικής που ουσιαστικά είναι αδύνατη η άμεση ή έστω εντός ωρών επαναλειτουργία του. Στην περίπτωση αυτή (ολικής καταστροφής) είναι απαραίτητη η ύπαρξη μιας εφεδρικής εγκατάστασης και ενος σχεδίου αποκατάστασης της λειτουργίας του νοσοκομείου σε αυτή την εγκατάσταση. Η εφεδρική εγκατάσταση μπορεί να βρίσκεται σε άλλο χώρο του νοσοκομείου, σε μια κινητή μονάδα παροχής υπηρεσιών Η/Υ, σε θυρίδα κτλ.

Το βέβαιο είναι ότι ένα λεπτομερές Σχέδιο Εκτακτής Ανάγκης πρέπει να συντάσσεται και να ελέγχεται σε πραγματικές συνθήκες, να δοκιμάζεται σε τακτά χρονικά διαστήματα και να αναθεωρείται όποτε αυτό είναι απαραίτητο.

4.1.2. Ασφάλεια στις καθημερινές διεργασίες.

Η μέριμνα της διοίκησης ενος νοσοκομείου και η πολιτική ασφάλειας πρέπει να επικεντρώνεται με εξ'ίσου, αν όχι και μεγαλύτερο βάρος, στην ασφάλεια κατά την διάρκεια της καθημερινής λειτουργίας των Π.Σ. Η συγκεκριμένη πολιτική ασφάλειας θα πρέπει να καλύπτει τα κτίρια, τις εγκαταστάσεις, το λογισμικό.Θα πρέπει παράλληλα να μεριμνά για το ποιοί και πώς αναπτύσσουν, συντηρούν ή χειρίζονται τα διάφορα Π.Σ. Ποιοί μπαίνουν σε ευαίσθητους χώρους και πώς διακινούνται οι εμπιστευτικές πληροφορίες εκτός δικτύων. Πώς και πόσες γενιές φυλάσσονται απο ποιά

δεδομένα και πού. Η συστηματική καταγραφή και παρακολούθηση όλων αυτών, αποτελεί μια βασικότατη,επίπονη και αρκετά εξειδικευμένη λειτουργία ελεγτικού και εμπιστευτικού χαρακτήρα. Η εποπτεία και ο έλεγχος της τήρησης των προδιαγραφών, η τακτική επιθεώρηση ή αναθεώρηση τους,και η λήψη κάποιων νέων μέτρων, πρέπει να είναι μια συνεχής και μόνιμη απασχόληση των υπευθύνων ασφαλείας που θα αποτελούν ξεχωριστή υπηρεσία στο κέντρο πληροφορικής με απ'ευθείας αναφορά στη διοίκηση. Σε γενικές γραμμές θα μπορούσε να διακριθεί η ασφάλεια των καθημερινών εργασιών σε ενα νοσοκομείο στις εξής λογικές ενότητες:

- Φυσική ασφάλεια των Π.Σ.
- Λογική ασφάλεια των Π.Σ.
- Ασφάλεια λοιπών δικτύων, περιφερειακού και βοηθητικού εξοπλισμού.

Στην συνέχεια παρατίθενται συνοπτικά, για κάθε προαναφερόμενη ενότητα οι συνιστώσες που πρέπει να προστατευθούν, οι κίνδυνοι και τα μέτρα που πρέπει να ληφθούν για την αποφυγή των αρνητικών συνεπειών, σε όλη την υλικοτεχνική υποδομή και χρήση ενος Π.Σ.

4.2. Φυσική ασφάλεια

➢ Προστασία των χώρων του Κέντρου Πληροφορικής και ιδιαίτερα του computer room (ελεγχόμενη είσοδο).

➢ Προστασία Υλικού (HARDWARE) από οποιαδήποτε απειλή, βλάβη ή ανθρώπινη απροσεξία.

➢ Προστασία των εφεδρικών αντιγράφων (back-up) του συστήματος και των προγραμμάτων εφαρμογών και των δεδομένων.

➢ Εγκατάσταση του συστήματος αδιάλειπτου λειτουργίας (U.P.S.) και συστήματος πυρόσβεσης με αδρανές αέριο.

Κίνδυνοι:

✓ Βλάβη ή καταστροφή υλικού (hardware).

✓ Απώλεια Δεδομένων.

✓ Αλλαγή δηλωμένων χαρακτηριστικών περιφεριακών συσκευών.

✓ Λανθασμένα Αποτελέσματα.

✓ Λανθασμένες εκτυπώσεις.

Μέτρα:

✓ Απαγόρευση μη εξουσιοδοτημένης πρόσβασης σε computer room, τερματικά, βιβλιοθήκες ταινιών, δίσκων.

✓ Πίνακες εξουσιοδότησης θα απεικονίζουν το δικαίωμα του χρήστη να έχει πρόσβαση σε δίσκους, ταινίες και αρχεία (πεδία αρχείων, εγγραφές αρχείων).

✓ Στατιστική παρακολούθηση παραβιάσεων.

✓ Προσεκτική επιλογή και σωστή διοικητική εποπτεία των εργαζομένων στο κέντρο πληροφορικής.

✓ Τήρηση ασφαλών δοκιμών προδιαγραφών με συστήματα πυρόσβεσης, πυρασφαλή φύλαξης αρχείων.

✓ Δημιουργία χώρων εργασίας με συνθήκες κατάλληλου φωτισμού, κλιματισμού.

4.3. Λογική ασφάλεια

- Προφύλαξη στο λογισμικό.
- Προφύλαξη στα δεδομένα.
- Προφύλαξη στο λογισμικό.
- Λειτουργικά προγράμματα.
- Προγράμματα εφαρμογών,πακέτα.
- Προστασία λειτουργίας μνήμης κεντρικής μονάδας επεξεργασίας (Κ.Μ.Ε.).
- Προστασία αρχείων λειτουργικού συστήματος.
- Προστασία βιβλιοθηκών εγκατάστασης.
- Προστασία-έλεγχος προσπέλασης.

Κίνδυνοι:

✓ Αλλοίωση των παραμέτρων configuration του συστήματος.

✓ Λογική απώλεια δίσκων, βιβλιοθήκων κ.λ.π.

✓ Ενεργοποίηση κρυμμένων λογικών επιλογών ('ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ', ¨ΛΟΓΙΚΕΣ ΒΟΜΒΕΣ¨).

✓ Ετεροπροσωπία.

✓ Παρακαμπτήρια εργαλεία.

✓ Αρπαγή συνθηματικού (password grabbers) των εξουσιοδοτημένων system programmers.

Μέτρα:

✓ Μηχανισμοί προστασίας μνήμης (π.χ.τεμαχισμό, σελιδοποίηση).

✓ Μηχανισμοί ελέγχου προσπέλασης (πίνακας ελέγχου προσπελάσεων).

✓ Μηχανισμοί προστασίας αρχείων.

✓ Εφεδρικά αντίγραφα (back-up) συστήματος.

✓ Συστήματα αδιάλειπτου λειτουργίας (U.P.S.) ή εφεδρικά αντίγραφα.

✓ Προγράμματα ανίχνευσης ιών.

✓ Ημερολόγια Κινήσεων όπου καταγράφονται όλες οι μεταβολές οι οποίες έχουν σχέση με την λειτουργία και την ασφάλεια του συστήματος.

- Προστασία προγραμμάτων εφαρμογών,πακέτων.
- Βιβλιοθήκες προγραμματισμού.
- Έλεγχος προσπέλασης.

Κίνδυνοι:

✓ «Καρφωτές» τροποποιήσεις (αφαίρεση της τροποοίησης μετά το τρέξιμο του προγράμματος).

✓ Παράνομη τροποποίηση μορφοποίησης (format) αρχείων, περιεχόμενων πεδίων.

✓ Διακοπές προγραμμάτων.

✓ Προσομοίωση και μεταβολή των λογισμικών

Μέτρα:

✓ Κλειδιά (passwords).

✓ Πίνακες ελέγχου προσπέλασης.

✓ Έξυπνες κάρτες.

✓ Εφαρμογή ειδικών πακέτων Ασφάλειας.

- Προφύλαξη στα δεδομένα.
- Προστασία ¨ευαίσθητων¨ δεδομένων (κρυπτογραφικός έλεγχος).
- Προστασία δεδομένων απο τυχαίες ή ηθελημένες διαγραφές ή αλλοιώσεις.
- Προστασία ροής δεδομένων (κοινό, εμπιστευτικό, μυστικό, απόρρητο).
- Προστασία βάσης δεδομένων

Κίνδυνοι:

Παράνομη αναζήτηση δεδομένων.

✓ Διαρροή πληροφοριών (κοινών ή απόρρητων), (data leakage)

✓ Τροποποίηση δεδομένων πριν τη καταχώρηση ή μετά.

✓ Τυχαία καταστροφή δεδομένων.

✓ Τυχαία ή σκόπιμη βλάβη βάσης δεδομένων (με αποτέλεσμα παράνομη τροποποίηση και διασύνδεση δεδομένων).

Μέτρα:

✓ Διαδικασία αλληλοεπιβεβαίωσης ταυτοποίηση-εξουσιοδότηση του οποιουδήποτε χρήστη επηρέζει τα δεδομένα.

✓ Χρήση κλειδιού (password) και ταυτότητας χρήστη (user ID).

✓ Υποχρεωτικοί έλεγχοι προσπέλασης.

✓ Κρυπτογραφικοί έλεγχοι προσπέλασης στα δεδομένα των αρχείων και στη μετάδοση δεδομένων.

✓ Πίνακες εξουσιοδότησης για κατηγορίες δεδομένων που ο χρήστης μπορεί να διαβάσει ή να γράψει.

✓ Τακτική λήψης εφεδρικών αντιγράφων (back-up).

✓ Χρήση πακέτων ασφαλείας.

Ένα θέμα το οποίο συσχετίζεται άμεσα με την προστασία των δεδομένων είναι οι εκτυπωμένες καταστάσεις οι οποίες εμφανίζουν τα δεδομένα.Θα πρέπει να ληφθούν ιδιαίτερα μέτρα για ασφαλή διακίνηση των εκτυπωμένων καταστάσεων ώστε να φθάνουν έγκαιρα στους εξουσιοδοτημένους υπαλλήλους. Ταυτόχρονα θα πρέπει, για μεγαλύτερη εμπιστευτικότητα, οι καταστάσεις να τυπώνονται σε τοπικό επίπεδο και δτις μονάδες κάθε υπηρεσίας και μόνο σε εξαιρετικές συνθήκες απο την κεντρική μονάδα εκτύπωσης.

4.4. Φυσική προστασία του δικτύου εγκατάστασης.

Κίνδυνοι:

✓ Υποκλοπή μηνυμάτων απο παγίδευση γραμμών.

✓ Τροποποίηση μηνυμάτων με παγίδευση γραμμών.

✓ Υποκλοπή παραμέτρων αυθεντικοποίησης.

✓ Λήψη ηλεκτρομαγνητικής ακτινοβολίας απο τα τερματικά.

✓ Βλάβη δικτύων.

Μέτρα:

✓ Κρυπτογραφία κατά την μεταφορά δεδομένων.

✓ Αποκλειστικές και εναλλακτικές τηλεφωνικές γραμμές.

✓ RESTART/RECOVERY διαδικασίες.

✓ Μέτρα για φυσική προστασία εγκατάστασης και συνιστωσών δικτύου.

4.5. Ασφάλεια λοιπών δικτύων περιφερειακού και βοηθητικού εξοπλισμού.

Στο κεφάλαιο αυτό εξετάζονται οι παράμετροι ασφαλείας που ισχύουν για τον λοιπό «μηχανογραφικό» εξοπλισμό που υποστηρίζει τις υπηρεσίες του νοσοκομείου είτε είναι συνδεδεμένες με κάποιας μορφής δίκτυο, είτε είναι αυτόνομοι μικροϋπολογιστές. Τα δίκτυα έχουν απο μόνα τους υψηλές προδιαγραφές ασφάλειας, η τήρηση των οποίων είναι απαραίτητη προϋπόθεση για την λειτουργία τους.

Τα δίκτυα όμως τα οποία εγκαθίστανται για την εξυπηρέτηση άλλων αναγκών (π.χ.οικονομικών στοιχείων, στοιχείων προσωπικού και λοιπών υπηρεσιών) χρήζουν ιδιαίτερης προσοχής.

Τέλος,υπάρχει και το δίκτυο των τερματικών για ανάπτυξη,υποστήριξη ή έλεγχο των εφαρμογών που απαιτεί ιδιαίτερη προσοχή απο πλευράς ασφάλειας.

Σε γενικές γραμμές πρέπει να αναπτυχθεί μια πολιτική ασφαλείας για αυτού του είδους του περιφερειακού εξοπλισμού «γραφείων» που θα εξασφαλίζει:

- Προστασία και έλεγχο του εξοπλισμού.
- Προστασία και έλεγχο του λογισμικού.
- Την κατηγοριοποίηση του βαθμού ασφαλείας των δεδομένων.
- Την κατηγοριοποίηση των προγραμμάτων που βρίσκονται εγκατεστημένα στον εξοπλισμά αυτό.

Τα παραπάνω πρέπει να τηρηθούν επιπλέον των μέτρων φυσικής ασφάλειας, πρόσβασης του προσωπικού που ισχύουν για το κέντρο πληροφορικής .

Κίνδυνοι:

- ✓ Μορφοποίηση δίσκου (formatting).
- ✓ Σβήσιμο αρχείων ή προγραμμάτων.
- ✓ Πλημμελείς διαδικασίες λήψης εφεδρικών αντιγράφων και αποθήκευση αρχείων.
- ✓ Ξεχασμένα κλειδιά ή μη εξουσιοδοτημένη προσπέλαση.
- ✓ Κίνδυνοι απο τους ιούς.

Μέτρα:

- ✓ Συστηματική λήψη εφεδρικών αντιγράφων (back-up).
- ✓ Χρήση έλεγχων προσπέλασης ή πακέτων ασφαλείας.
- ✓ Χρήση "κρυμμένων αρχείων".
- ✓ Εκπαίδευση των χρηστών σε τεχνικές προστασίας.
- ✓ Χρήση προγραμμάτων ανίχνευσης ιών (Anti-virus).
- ✓ Φύλαξη των εμπιστευτικών αρχείων σε δισκέτες σε ασφαλή χώρο.
- ✓ Φυσική προστασία του χώρου του PC, των περιφερειακών και βοηθητικών συσκευών.

4.6. ΑΣΦΑΛΕΙΑ ΝΟΣΟΚΟΜΕΙΑΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ-ΕΛΕΓΧΟΣ

Έλεγχος λειτουργίας κέντρου πληροφορικής.

Η επιβεβαίωση ότι όντως έχουν ληφθεί τα απαραίτητα μέτρα για την ασφάλεια και την καλή λειτουργία όλων των συνιστωσών του κέντρου πληροφορικής (Υλικού-Λογισμικού) εξασφαλίζεται με τον ελεγχό του (Auditing).

Οι διαδικασίες ελέγχων του κέντρου πληροφορικής στα περισσότερα νοσοκομεία δεν έχουν αναπτυχθεί πλήρως. Ο έλεγχος επικεντρώνεται:

- ✓ Στη φυσική προστασία του κέντρου πληροφορικής.
- ✓ Στην αποθήκευση "των προϊόντων" του κέντρου.
- ✓ Στο σχέδιο έκτακτης ανάγκης.
- ✓ Στην ύπαρξη υπηρεσίας ασφαλείας.
- ✓ Στα δίκτυα.
- ✓ Στην προστασία του λογισμικού (Λ.Σ. προγραμμάτων εφαρμογών, πακέτων).
- ✓ Στην Τεκμηρίωση των προγραμμάτων.
- ✓ Στην προστασία των δεδομένων.

Στην συνέχεια ακολουθεί μια μικρή αναφορά σε κάθε μια από τις προαναφερόμενες περιοχές ελέγχου:

Φυσική προστασία του κέντρου πληροφορικής

Έλεγχος αν υπάρχουν διαδικασίες που εγγυώνται την φυσική προστασία του κέντρου πληροφορικής π.χ. Προσωπικό ασφάλειας, Σύστημα ελέγχου πρόσβασης, Κλειδαριές ασφάλειας, πυρασφάλιση, Κλιματισμός, U.P.S.

Αποθήκευση "των προιόντωντου" κέντρου

Έλεγχος π.χ. :

--Εάν υπάρχει έλεγχος εξουσιοδοτημένης πρόσβασης.

--Εαν υπάρχουν ετικέτες στις ταινίες

--Εαν υπάρχει βιβλιοθήκη ταινιών

--Εαν υπάρχουν οδηγίες διατήρησης και καταστροφής αρχείων.

Σχέδιο έκτακτης ανάγκης

Έλεγχος π.χ.:

--Εάν υπάρχει σχέδιο.

--Εάν δοκιμάζεται σε τακτά χρονικά διαστήματα.

--Εάν παρουσιάζει παραλείψεις ή μειονεκτήματα.

--Εάν υπάρχει καθορισμός αρμοδιτήτων και εξουσιοδοτήσεων σε περίπτωση ενεργοποίησης του σχεδίου έκτακτης ανάγκης.

Ύπαρξη υπηρεσίας ασφάλειας

--Εαν υπάρχει υπεύθυνος ασφάλειας και αντίστοιχη υπηρεσίας.

Δίκτυα

--Οι ελεγκτές είναι επιφυλακτικοί στον έλεγχο δικτύων λόγο των εξειδικευμένων τεχνικών γνώσεων που απαιτούνται.Θα πρέπει όμως οπωσδήποτε να γίνεται έλεγχος της ασφάλειας και της καλής λειτουργίας των δικτύων διότι αποτελούν βασικό τμήμα του όλου πληροφορικού κέντρου και άπτονται κρίσιμων εφαρμογών.

Προστασία του Λογισμικού (Λ.Σ, προγραμμάτων-Εφαρμογών, Πακέτων).

Έλεγχος π.χ:

--Εαν υπάρχει ενσωματωμένος έλεγχος ασφάλειας.

--Εαν υπάρχει διαχωρισμός αρμοδιοτήτων όπως:

1. Στην ανάπτυξη εφαρμογών

2. Στην ενημέρωση αρχείων

3. Στην λειτουργία του εξοπλισμού.

--Εάν υπάρχει έλεγχος εξουσιοδότησης (Διάβασμα, Γράψιμο, Εκτελεση).

--Εάν υπάρχει έλεγχος πληρότητας εισαγόμενων δεδομένων.

--Εάν υπάρχει έλεγχος αυτόματης παραγωγής κινήσεων.

--Εαν υπάρχει έλεγχος συνεχόμενων εκδόσεων προγραμμάτων.

Τεκμηρίωση των προγραμμάτων

Έλεγχος εαν υπάρχει π.χ:

Η δομή των αρχείων και των βάσεων δεδομένων.

--Η δομή των εισερχομένων στοιχείων και των εξερχομένων αποτελεσμάτων.

--Υπολογισμοί τύπων

--Ακριβείς αναφορά στις υπάρχουσες οθόνες

--Εκτύπωση του κώδικα προγραμμάτων με όλες τις τροποποίησεις τους

Προστασία των δεδομένων

Εαν υπάρχουν διαδικασίες που να υποστηρίζουν:

--Έλεγχο εισόδου δεδομένων (Πηγής-Εξουσιοδότησης)

--Έλεγχο πληρότητας δεδομένων

--Έλεγχο των απορρίψεων του συστήματος

--Έλεγχο αποφυγής διπλής καταχώρησης εγγράφων.

--Έλεγχο υπολογισμού αποτελεσμάτων κρίσιμων εφαρμογών (Εξόδου Δεδομένων)

--Έλεγχο λήψης εφεδρικών αντιγράφων (ή Backup) δεδομένων λειτουργικού συστήματος και προγραμμάτων εφαρμογών.

--Έλεγχο ότι όντως είναι επαρκής η διαδικασία λήψεως εφεδρικών αντιγράφων

Εάν υπάρχουν οδηγίες γαι τις γενιές διατήρησης των εφεδρικών αντιγράφων.

Εάν υπάρχουν οδηγίες για την επανάκτηση των δεδομένων του συστήματος στη περίπτωση ύπαρξης προβλήματος.

Εάν υπάρχουν διαδικασίες που να εξασφαλίζουν τον έλεγχο στον πίνακα εξουσιοδότησης για αναζήτηση ή τροποποίηση των "ευαίσθητων" δεδομένων.

4.7. ΤΕΧΝΙΚΕΣ ΕΛΕΓΧΟΥ

Οι προαναφερόμενοι έλεγχοι υλοποιούνται απο τον ελεγκτή ασφάλειας είτε με χειρόγραφες διαδικασίες είτε με την χρήση προγραμμάτων ή άλων πακέτων ελέγχου.

Η χρήση χειρόγραφης τεχνικής ελέγχου ή μηχανογραφικής (προγράμματα-πακέτα ελέγχου) εξαρτάται απο την φύση της ελεγχόμενης διαδικασίας αλλά και απο τη διαθεσιμότητα ή όχι μηχανογραφικών μέσων ελέγχου.

Στη συνέχεια αναφέρουμε τις πιο συνιθισμένες χειρόγραφες και αυτοματοποιημένες τεχνικές.

4.7.1.Χειρόγραφες τεχνικές

1) Ερωτηματολόγιο:

Χρησιμοποιείται σε μεγάλη κλίμακα για έλεγχο που σχετίζεται π.χ.

-Με εμπιστευτικά προγράμματα

-Με ακρίβεια αποτελεσμάτων

-Με την ασφάλεια του Λ.Σ.

-Με την τεκμηρίωση των προγραμμάτων

4.7.2. Είδικοι έλεγχοι

Π.χ.

-Στο ημερολόγιο κινήσεων του χειριστή,του υπευθύνου ασφάλειας.

-Στους πίνακες εξουσιοδότησης

-Στα ημερολόγια καταγραφής προσπελάσεων.

4.7.3. Αυτοματοποιημένες τεχνικές

Παράλληλη προσομοίωση:

Γίνεται έλεγχος σε ορισμένα τμήματα της εφαρμογής,δημιουργείται πρόγραμμα το οποίο τρέχει παράλληλα με την κανονική ροή και έχει σαν σκοπό την εξαγωγή των ίδιων αποτελεσμάτων. Σε αντίθετη περίπτωση γίνεται μελέτη των διαφορετικών αποτελεσμάτων.

4.7.4. Μέθοδος ενσωματωμένου ελέγχου:

Η μέθοδος ενσωματωμένου ελέγχου είναι η παλαιότερη μέθοδο ελέγχου κατά την οποία δημιουργείται μια σμικρογραφία της ελεγχόμενης επεξεργασίας. Τα δοκιμαστικά δεδομένα ελέγχονται παράλληλα με την κανονική επεξεργασία χωρίς να αναμιγνύονται.

4.8. Σημεία ελέγχου των πληροφοριακών συστημάτων.

4.8.1. Έλεγχος πρόσβασης στο Υπολογιστικό κέντρο

- Θα πρέπει να υπάρχει ασφαλής τρόπος πρόσβασης ελέγχου στο υπολογιστικό κέντρο .
- Θα πρέπει να υπάρχει πρόβλεψη εάν οι επισκέπτες έχουν ή όχι ελεύθερη πρόσβαση.

- Θα πρέπει να υπάρχει σχέδιο εάν η μετακίνηση των επισκεπτών ειναι περιορισμένη ή ελεγχόμενη.

4.8.2. Έλεγχος Πρόσβασης στο κέντρο Επικοινωνιών

- Θα πρέπει να είναι ικανοποιητικά προστατευμένες οι περιοχές που παρέχουν ηλεκτρονική επικοινωνία για το υπολογιστικό κέντρο.
- Ο κλιματισμός θα πρέπει να είναι ικανοποιητικός για τον εξοπλισμό του κέντρου επικοινωνιών και του προσωπικού.
- Θα πρέπει να υπάρχει καλή ηλεκτρική παροχήμε εφεδρικές μπαταρίες και μονάδες προστασίας απο πτώσεις και ανορθώσεις τάσης.
- Θα πρέπει να υπάρχουν κλειδαριές σε όλους τους Τηλ.Θαλάμους.
- Θα πρέπει να υπάρχουν συναγερμοί στα κύρια δωμάτια επικοινωνιών.
- Θα πρέπει να υπάρχουν δρομολογημένες πολλαπλές γραμμές για τις πιο σημαντικές λειτουργίες επικοινωνίας.
- Θα πρέπει να υπάρχει ένα οργανόγραμμα που να αναφέρει ποιος είναι ο ακριβής ρόλος των εργαζομένων.

4.8.3. Έλεγχος πρόσβασης στους υπολογιστικούς πόρους

- Θα πρέπει το λογισμικό και η τεκμηρίωση να κρατούνται σε μια σίγουρη και ασφαλή θέση.
- Θα πρέπει να υπάρχουν αντίγραφα για το λογισμικό και την τεκμηρίωση στην περίπτωση κάποιας καταστροφής.Η πρόσβαση στο λογισμικό και στην τεκμηρίωση θα πρέπει να απαιτεί κάποιες ιδιαίτερες γνώσεις.
- Σε περίπτωση αλλοίωσης ή καταστροφής στο λογισμικό θα πρέπει να δικαιολογούνται οι αλλαγές.
- Θα πρέπει να χρησιμοποιούνται κωδικοί πρόσβασης οι οποίοι θα ελέγχονται περιοδικά.
- Οι χρήστες τερματικών θα πρέπει να χρησιμοποιούν κλειδιά.
- Το λειτουργικό σύστημα πρέπει να έχει ενσωματωμένο μηχανισμό προστασίας για τη ανεξέλεκτη χρήση Λογισμικού Ασφαλείας.
- Το λογισμικό ασφαλείας θα πρέπει να παρέχει έλεγχο πρόσβασης πολλών επιπέδων για τα αρχεία και τις Β.Δ.

- Οι προγραμματιστικές αλλαγές θα πρέπει να ελέγχονται και να τεκμηριώνονται.

4.8.4. Προστασία απο φωτιά

- Οι πόρτες, οι τοίχοι, επίπλωση θα πρέπει να είναι κατασκευασμένα απο υλικά που αντέχουν στη φωτιά.
- Θα πρέπει να εγκατασταθούν συσκευές ανίχνευσης καπνού και θερμότητας, οι οποίες αν είναι δυνατόν να απενεργοποιούν αυτόματα τον κλιματισμό.
- Το εύλεκτο δεν πρέπει να βρίσκεται κοντά στο υπολογιστικό κέντρο.
- Θα πρέπει να απαγορέυται το κάπνισμα.
- Θα πρέπει να υπάρχουν πυροσβεστικά σημεία, πυροσβεστήρες και εξειδικευμένο προσωπικό στη πυρόσβεση.
- Θα πρέπει να υπάρχουν διακόπτες ισχύος για επίγουσες περιπτώσεις, όπως επίσης και ασφαλιστική κάλυψη για την περίπτωση ζημιάς απο φωτιά.

4.8.5. Προστασία απο πλημμύρα

- Θα πρέπει να υπάρχουν αγωγοί απομάκρυνσης του νερού καθώς και τα απαραίτητα μέτρα προστασίας για τις διαρροές του νερού.
- Θα πρέπει να υπάρχει ασφαλιστική κάλυψη στην περίπτωση ζημιάς απο νερό.

4.8.6. Παροχή ισχύος

Το κέντρο δεδομένων θα πρέπει να βρίσκεται σε κάποιο μέρος όπου η παροχή ισχύος θεωρείται αξιόπιστη.

Το χρονικό διάστημα που απαιτείται για την επαναφορά στην περίπτωση της πτώσης τάσης πρέπει να είναι ελάχιστο,ενώ παράλληλα πρέπει να υπάρχουν εφεδρικές μπαταρίες μέχρις ότου επανέλθει η τάση του ρεύματος.Θα πρέπει να υπάρχει μια πολιτική για την αντιμετώπιση των πιθανών επιπτώσεων που θα εμφανιστούν στην ηλεκτρική παροχή λόγω του "βαρέος" εξοπλισμού ή άλλων αιτιών.

Κλιματισμός

Το κέντρο δεδομένων πρέπει να έχει το δικό του σύστημα κλιματισμού, επίσης πρέπει να υπάρχουν και εφεδρικά στοιχεία κλιματισμού τα οποία πρέπει να ελέγχουν την θερμοκρασία και υγρασία.

4.8.7. Προσωπικές θεωρήσεις

- Θα πρέπει να υπάρχει κάποιος υπεύθυνος για την ασφάλεια των υπολογιστών με ξεκάθαρες και καθορισμένες αρμοδιότητες.
- Θα πρέπει να υπάρχουν πολιτικές και διαδικασίες που σχετίζονται με την ασφάλεια των υπολογιστών.
- Το προσωπικό θα πρέπει να είναι καλά εκπαιδευμένο έστι ώστε να καταλαβαίνει τις πολιτικές και διαδικασίες ασφάλειας,ενώ ταυτόχρονα θα πρέπει να έχει συνειδητοποιήσει τη σπουδαιότητα της ασφάλειας.
- Θα πρέπει να κρατιούνται πληροφορίες για όλους τους επισκέπτες που χρησιμοποιούν το κέντρο δεδομένων.
- Θα πρέπει να γίνεται έλεγχος του ιστορικού των προμηθευτών.
- Όταν ένας υπάλληλος αλλάζει θέση ή απολύεται πρέπει να γίνονται αλλαγές στα κλειδιά ώστε να μην μπορεί να έχει πρόσβαση.

4.8.8. Σχέδιο Επαναφοράς

- Θα πρέπει να υπάρχει κάποιος υπεύθυνος που θα κατευθύνει τις διαδικασίες επαναφοράς απο κάποια καταστροφή με καθορισμένες και ξεκάθαρες αρμοδιότητες.
- Θα πρέπει να έχει προβλεφθεί η ύπαρξη ενός εφεδρικού κέντρου δεδομένων στο σχέδιο επαναφοράς και να έχει ελεγχεί και δοκιμαστεί με τις κρίσιμες εφαρμογές.
- Θα πρέπει να υπάρχου επιπλέον αντίγραφα των σημαντικών αρχείων, των αρχείων και των βάσεων δεδομένων, του πηγαίου κώδικα των προγραμμάτων, τα τμήματα των προγραμμάτων και της τεκμηρίωσής του τα οποία να φυλάγονται μακριά απο το κέντρο δεδομένων.
- Θα πρέπει να υπάρχουν αντίγραφα του Λ.Σ και των άλλων συστημάτων λογισμικού, που είναι απαραίτητα για την δημιουργία του κανονικού λειτουργικού περιβάλλοντος στο εφεδρικό κέντρο δεδομένων.

- Θα πρέπει να υπάρχουν διαδικασίες επαναφοράς όταν συμβαίνουν λειτουργικά λάθη, τα οποία μπορεί να καταστρέψουν πολύτιμα δεδομένα-προγράμματα.

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ

Επιπτώσεις από την Έλλειψη Ασφάλειας και Ελέγχου σε ένα Νοσοκομείο.

Περίληψη 5ου κεφαλαίου.

Η εξέλιξη των υπολογιστικών συστημάτων και η συνεχής αύξηση των απαιτήσεων των χρηστών οδήγησαν στην εμφάνιση των *δικτύων υπολογιστικών συστ*ημάτων. Τα *δίκτυα* επέτρεψαν την καλύτερη αξιοποίηση των συστημάτων αυξάνοντας τις δυνατότητες τους και την επικοινωνία των χρηστών από μεγάλες αποστάσεις. Παράλληλα, με την ανάπτυξη των δικτύων, παρουσιάστηκε η ανάγκη προστασίας των χρηστών και των δεδομένων που μεταδίδονται ή αποθηκεύονται. Στο κεφάλαιο αυτό γίνεται μια λεπτομερής αναφορά στα διάφορα είδη *δικτύων* που υπάρχουν και την ασφάλεια που παρέχουν όταν γίνεται διακίνηση *Ιατρικών Πληροφοριών* οι οποίες χαρακτηρίζονται ως δεδομένα *υψηλής ευπάθειας*. Συνεπώς κατά τη διακίνηση των Ιατρικών πληροφοριών μέσω των δικτύων οποιαδήποτε παρεμβολή **μη εξουσιοδοτημένη** αλλοιώνει το περιεχόμενο τους.

5.1. Μέθοδοι προστασίας υπολογιστικών συστημάτων.

Υπάρχουν τέσσερις βασικές μέθοδοι για την προστασία της ασφάλειας των υπολογιστικών συστημάτων:

Α) Έλεγχοι προσπέλασης συστήματος

Εξασφάλιση ότι μη εξουσιοδοτημένοι χρήστες δεν εισέρχονται στο σύστημα. Ενθάρρυνση (και κάποιες φορές εξαναγκασμός) των εξουσιοδοτημένων χρηστών να είναι συνειδητοποιημένοι σε ότι αφορά την ασφάλεια, αλλάζοντας τα συνθηματικά τους συχνά. Το σύστημα προστατεύει επίσης τις πληροφορίες για τα συνθηματικά και καταγράφει ποιος κάνει τι στο σύστημα, ειδικά όταν γίνεται κάτι σχετικό με την ασφάλεια (είσοδος στο σύστημα, άνοιγμα αρχείου, χρήση ειδικών προνομίων).

Β) Έλεγχος προσπέλασης πληροφοριών

Παρακολούθηση και έλεγχος ποιος έχει προσπέλαση σε ποιου είδους πληροφορίες και γιατί. Εάν το σύστημα υποστηρίζει "κατά διάκριση" ελέγχους προσπέλασης (discretionagy access control), μπορεί να καθοριστεί, εάν άλλα άτομα μπορούν να διαβάσουν ή να μεταβάλλουν τις πληροφορίες ενός χρήστη. Το σύστημα μπορεί να υποστηρίζει και 'κατά απαίτηση' ελέγχους προσπέλασης (mandatory access control), ώστε να καθορίζονται από το σύστημα οι κανόνες προσπέλασης βάση των ετικετών ασφαλείας (security labels) των ατόμων, και των άλλων αντικειμένων του συστήματος.

Γ) Διαχείριση του συστήματος και της ασφάλειας του

Εκτέλεση off-line των διαδικασιών που αποτελούν ή επιτυγχάνουν ρήγμα στην ασφάλεια ενός συστήματος: διαγράφοντας διοικητικές ευθύνες του συστήματος με ασφάλεια, εκπαιδεύοντας κατάλληλα τους υπαλλήλους και παρακολουθώντας τους χρήστες για να επιβεβαιωθεί η τήρηση των πολιτικών ασφαλείας. Αυτή η κατηγορία συνεπάγεται, επίσης, πιο γενικές μορφές διαχείρισης της ασφάλειας, όπως τον υπολογισμό των απειλών που αντιμετωπίζει η ασφάλεια του συστήματος και του κόστους προστασίας από αυτές.

Δ) Σχεδίαση του συστήματος

Η εκμετάλλευση των βασικών χαρακτηριστικών του υλικού και λογισμικού εξοπλισμού (η χρήση μιας αρχιτεκτονικής που μπορεί να τμηματοποιεί τη μνήμη) οδηγεί στην απομόνωση προνομιακών διαδικασιών από μη προνομιακές διαδικασίες.

Είναι σίγουρο ότι το υπολογιστικό έγκλημα θα συνεχίσει να υπάρχει. Ο στόχος της ασφάλειας υπολογιστικού περιβάλλοντος είναι να θεσπίσει ελέγχους, που να διατηρούν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Κάποιες φορές αυτοί οι έλεγχοι είναι ικανοί να αναχαιτίσουν επιθέσεις, ενώ άλλοτε καταφέρνουν μόνο να εντοπίσουν μια εισβολή κατά τη διάρκεια της ή αφότου έχει συμβεί.

5.2. Είδη ελέγχων

Τα βασικά είδη ελέγχων που προσπαθούν να εμποδίσουν την εξάπλωση των ευπαθειών ενός υπολογιστικού συστήματος εμπίπτουν στις ακόλουθες κατηγορίες.

5.2.1.Κρυπτογράφηση

Το ισχυρότερο εργαλείο της παροχής ασφάλειας σε ένα υπολογιστικό περιβάλλον είναι η κωδικοποίηση. Μεταμορφώνοντας τα δεδομένα, ώστε να δείχνουν άσχετα σε οποιονδήποτε τα παρατηρεί εκτός του συστήματος, η αξία μιας υποκλοπής και η πιθανότητα τροποποίησης σχεδόν μηδενίζεται.

Ένα κρυπτογραφικό σύστημα (cryptographic system cryptosystem) έχει πέντε συνθετικά στοιχεία:

Α. ένα διάστημα μηνύματος απλού κειμένου (plaintext message space) m.

Β. ένα διάστημα κρυπτογραφημένου κειμένου (ciphertext message space) c.

Γ. ένα διάστημα κλειδί (key space) k.

Δ. μια 'οικογένεια' μετατροπών κρυπτογράφησης (family of enciphering transformations) Ek.

Ε. μια 'οικογένεια' μετατροπών αποκρυπτογράφησης (family of deciphering transformations) Dk.

Τα συστήματα κρυπτογράφησης κατηγοριοποιούνται:

- Ως συμμετρικά ή ενός κλειδιού, όπου τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι όμοια, ή εύκολα καθορίζονται το ένα για το άλλο.

- Ως μη συμμετρικά ή δυο κλειδιών.

Τα συστήματα ενός κλειδιού παρέχουν ένα πολύ καλό τρόπο κρυπτογράφησης των ιδιωτικών αρχείων των χρηστών. Κάθε χρήστης έχει ιδιωτικές μετατροπές για κρυπτογράφηση και αποκρυπτογράφηση αρχείων. Εάν οι υπόλοιποι χρήστες δεν μπορούν να έχουν προσπέλαση σε ένα από τα στοιχεία εξασφαλίζεται η μυστικότητα και η αυθεντικότητα των δεδομένων.

Στα μη συμμετρικά (ή δύο κλειδιών) συστήματα κρυπτογράφησης, τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης διαφέρουν, έτσι ώστε τουλάχιστον ένα κλειδί να μην μπορεί να προκύψει υπολογιστικά από το άλλο. Έτσι, η μια από τις μετατροπές μπορεί να αποκαλυφθεί χωρίς να θέτει σε κίνδυνο την άλλη. Η έννοια των κρυπτογραφικών συστημάτων δύο κλειδιών προτάθηκε από τους DIFFIE και HELMAN το 1976.Οι ίδιοι πρότειναν μια νέα μέθοδο κρυπτογράφησης που ονομάζεται κρυπτογράφηση δημόσιου κλειδιού (Public Key Ensryption), όπου κάθε χρήστης έχει και ένα δημόσιο κλειδί (Public Key) και ένα ιδιωτικό κλειδί (Private Key) και οι δύο χρήστες μπορούν να επικοινωνούν γνωρίζοντας ο ένας το δημόσιο κλειδί του άλλου.

Σε ένα σύστημα δημοσίου κλειδιού, κάθε χρήστης έχει μια μετατροπή δημόσιας κρυπτογράφησης, που μπορεί να καταγράφεται σε ένα δημόσιο κατάλογο (Public Directory) και μια ιδιωτική μετατροπή αποκρυπτογράφησης (Private Decipaghering Transformation) που είναι γνωστή μόνο στο χρήστη. Η ιδιωτική μετατροπή περιγράφεται από ένα ιδιωτικό κλειδί και η δημόσια περιγραφή από ένα δημόσιο κλειδί που προκύπτει από ένα ιδιωτικό κλειδί από μια μονόδρομη διαδικασία. Σε ένα σύστημα δημοσίου κλειδιού η μυστικότητα και η αυθεντικότητα παρέχονται από ξεχωριστές μετατροπές.

Η κρυπτογράφηση παρέχει μυστικότητα για τις πληροφορίες (Δεδομένα). Επιπροσθέτως, βοηθά στην παροχή ακεραιότητας (Αφού οι πληροφορίες που δεν μπορούν να αναγνωστούν άμεσα δεν μπορούν και να μεταβληθούν). Η κρυπτογράφηση είναι επίσης σημαντική για τα

πρωτόκολλα, μερικά από τα οποία διασφαλίζουν την διαθεσιμότητα των πόρων του συστήματος. Για τους παραπάνω λόγους, η κρυπτογράφηση βρίσκεται στο επίκεντρο των μεθόδων που χρησιμοποιούνται για την διασφάλιση των τριών στόχων της ασφάλεια υπολογιστικών συστημάτων. Δεν επιλύει πάντως όλα τα προβλήματα ασφαλείας ενός συστήματος.

5.2.2. Έλεγχοι Λογισμικού

Τα ίδια τα προγράμματα είναι ο δεύτερος συνδετικός κρίκος στην ασφάλεια των υπολογιστικών συστημάτων. Τα προγράμματα δεν πρέπει να είναι αρκετά ασφαλή μόνο για να αποκλείουν την εισβολή ατόμων εκτός του συστήματος, αλλά και να έχουν αναπτυχθεί και διατηρηθεί έτσι ,ώστε να μπορεί ναι είναι σίγουρος ο χρήστης για την αξιοπιστία τους. Οι έλεγχοι των προγραμμάτων περιλαμβάνουν:

- Ελέγχους Ανάπτυξης. Είναι τα πρότυπα βάση των οποίων ένα πρόγραμμα σχεδιάζεται, κωδικοποιείται , δοκιμάζεται και διαφυλάσσεται.

- Έλεγχος Λειτουργικών Συστημάτων. Υπάρχουν περιορισμοί που επιβάλλονται από το λειτουργικό σύστημα για να προστατεύεται ο κάθε χρήστης από τους άλλους χρήστες.

- Εσωτερικοί Έλεγχοι Προγραμμάτων. Υποστηρίζουν τους περιορισμούς ασφαλείας , όπως οι περιορισμοί πρόσβασης σε ένα DBMS.

- Οι έλεγχοι λογισμικού μπορούν να χρησιμοποιήσουν μέσα, όπως τμήματα υλικού, κρυπτογράφηση ή συλλογή πληροφοριών. Επηρεάζουν άμεσα τους χρήστες και για αυτό πρέπει να σχεδιάζονται προσεκτικά.

5.2.3. Έλεγχοι Υλικού

Πολυάριθμες συσκευές έχουν εφευρεθεί για να ενισχύσουν την ασφάλεια ενός υπολογιστικού περιβάλλοντος. Κυμαίνονται από υλική υλοποίηση της μεθόδου της κρυπτογράφησης, σε κλειδώματα που περιορίζουν την πρόσβαση, σε προστασίες κλοπής και σε συσκευές για την εξακρίβωση της ταυτότητα του εκάστοτε χρήστη.

5.2.4.Πολιτικές Ασφαλείας

Μερικοί άλλοι έλεγχοι είναι επίσης θέματα της ασφάλειας. Δεδομένου του παραπάνω γενικού πλαισίου και του ορισμού της ασφάλειας υπολογιστικών συστημάτων, μια πολιτική ασφάλειας καθορίζει :

- Ποίοι δίαυλοι επικοινωνίας μεταξύ των χρηστών (ή ομάδων τους) μπορούν να δημιουργηθούν.

- Τις απαιτήσεις για διαθεσιμότητα συγκεκριμένων εργαλείων–Ενεργειών επί των διαύλων αυτών.

- Τις απαιτήσεις για καθορισμό των κανόνων διάκρισης και μη έμμεσης προσπέλασης των διαύλων αυτών.

- Σύμφωνα με τα παραπάνω μπορούμε να διακρίνουμε τρεις βασικές πολιτικές ασφάλειας.

Α. Η πολυεπίπεδη πολιτική ασφάλειας(Multilevel). Προέρχεται από την παραδοσιακή τακτική χωρίς την χρήση Η/Υ. Η ανάγκη για μια τέτοια πολιτική προκύπτει, όταν ένα υπολογιστικό σύστημα περιέχει πληροφορίες με πληθώρα βαθμών εμπιστευτικότητας και έχει χρήστες που δεν έχουν εξουσιοδότηση για τον ανώτατο βαθμό εμπιστευτικότητας των πληροφοριών που περιέχονται στο σύστημα. Η προσέγγισή της βασίζεται στις ακόλουθες προϋποθέσεις (Δομικά στοιχεία): Υπάρχει ένας αριθμός χρηστών, ένα σύνολο από δεδομένα και ένα δικτυωτό ετικετών ασφαλείας.

Β. Η "Κατά διάκριση" ή εμπορική πολιτική ασφάλειας. Τα κατά διάκριση μοντέλα ελέγχου προσπέλασης εφαρμόζονται στα σημερινά συστήματα για να υποστηρίξουν μια συγκεκριμένη πολιτική ελέγχου προσπέλασης. Αυτή η προσέγγιση στηρίζεται στα ακόλουθα δομικά στοιχεία: Υπάρχει ένας αριθμός χρηστών, ένας αριθμός παραστατικών προς εκτέλεση και ένα σύνολο από δεδομένα.

Γ. Η πολιτική ασφάλειας της προσωπικής γνώσης. Η πολιτική ασφάλειας της προσωπικής γνώσης αναπτύχθηκε πρόσφατα και δίνει απόλυτη προτεραιότητα στην προστασία της ιδιωτικότητας. Από τεχνική άποψη συνδυάζει τις τεχνικές των συσχετιστικών Βάσεων Δεδομένων του αντικειμενοστραφούς προγραμματισμού και των Capability Based πληροφοριακών συστημάτων.

5.2.5. Έλεγχοι Φυσικού Επιπέδου

Οι έλεγχοι φυσικού επιπέδου είναι από τις ευκολότερες, τις ποιο αποδοτικές και λιγότερο δαπανηρές μεθόδους ελέγχου (Κλειδαριές στις πόρτες, Φρουροί, εφεδρικά αντίγραφα).

5.3. Αποτελεσματικότητα των ελέγχων

Η αποτελεσματικότητα των ελέγχων εξαρτάται από την ορθότητα της χρησιμοποίησής τους. Κάποιοι παράγοντες που επηρεάζουν την αποτελεσματικότητά τους είναι:

- Επίγνωση του μεγέθους του προβλήματος. Οι άνθρωποι που χρησιμοποιούν τους ελέγχους πρέπει να έχουν πειστεί για την ανάγκη για ασφάλεια.

- Πιθανότητα χρήσης. Κανένας έλεγχος δεν αποδίδει σωστά αν πρώτα δεν χρησιμοποιείται σωστά. Αυτό μπορεί να εκφραστεί με την ακόλουθη αρχή που καλείται "Αρχή της αποτελεσματικότητας" και λέει ότι "Οι έλεγχοι πρέπει να χρησιμοποιούνται για είναι αποτελεσματικοί και να είναι ικανοί ευκολόχρηστοι και κατάλληλοι". Η παραπάνω αρχή υπονοεί ότι οι έλεγχοι πρέπει ναι είναι αρκετά αποδοτικοί σε ότι αφορά χρόνο, χώρο μνήμης, ανθρώπινη δραστηριότητα, ή άλλους πόρους που χρησιμοποιούνται, ώστε η χρήση του ελέγχου να μην επηρεάζει την εργασία που προστατεύει. Επίσης, πρέπει να είναι επιλεκτικοί με τέτοιο τρόπο, ώστε να μην αποκλείονται οι εξουσιοδοτημένες προσπελάσεις. Διάφοροι τύποι ελέγχων μπορούν να εφαρμοστούν για τα σημεία όπου το σύστημα είναι εκτεθειμένο. Για παράδειγμα, το σύστημα ασφάλειας ενός μικροϋπολογιστικού συστήματος μπορεί να αποτελείται από ένα συνδυασμό ελέγχων της προσπέλασης των προγραμμάτων στα δεδομένα, της φυσικής πρόσβασης στον μικροϋπολογιστή και στα μέσα αποθήκευσης, ακόμη και του κλειδώματος αρχείων για να ελεγχθεί η προσπέλαση στα προγράμματα που βρίσκονται σε εξέλιξη.

- Περιοδικές αναθεωρήσεις. Ελάχιστο ποσοστό των ελέγχων είναι μόνιμα αποδοτικό. Συνεπώς, η αμφισβήτηση της αποτελεσματικότητας ενός ελέγχου πρέπει να είναι συνεχείς.

5.3.1. Δυνατότητα ελέγχου

Σε κάποιες εφαρμογές μπορεί να είναι επιθυμητή η παραγωγή μιας εγγραφής ελέγχου όλων των προσπελάσεων (ανάγνωσης ή εγγραφής) σε μια βάση δεδομένων. Μια τέτοια εγγραφή μπορεί να βοηθήσει στην διατήρηση της ακεραιότητας της βάσης, ή τουλάχιστον, στο να αποκαλυφθεί αργότερα ποιος πείραξε ποια πεδία και πότε.

Ένα δεύτερο πλεονέκτημα, που θα συζητηθεί αργότερα, ισχύει όταν οι χρήστες καταφέρνουν να έχουν έμμεση προσπέλαση. Καμία προσπέλαση ξεχώρισα δεν αποκαλύπτει πληροφορίες χρήζουσες προστασίας, αλλά ένα σύνολο προσπελάσεων αποκαλύπτει πληροφορίες όπως τα ξεχωριστά στοιχεία λύνου ένα μυστήριο. Σε αυτή την περίπτωση, ένας στενός και μυστικός έλεγχος θα χρησίμευε στην αναγνώριση των στοιχείων που έχουν ήδη δοθεί σε ένα χρήστη, σαν γνώμονας εάν θα έπρεπε να του δοθούν περισσότερα.

Ο καθορισμός των δομικών στοιχείων αποτελεί απαραίτητο τόλμημα για τον έλεγχο.

Ενώ, τα γεγονότα στα λειτουργικά συστήματα είναι συνήθως του τύπου 'άνοιξε αρχείο' ή 'κάλεσε διαδικασία', σπάνια είναι τόσο συγκεκριμένα όπως 'γράψε εγγραφή' ή 'εκτέλεσε εντολή'. Για να είναι χρήσιμοι οι έλεγχοι για τους προαναφερθέντες σκοπούς, οι έλεγχοι των βάσεων πρέπει να περιλαμβάνουν προσπελάσεις σε εγγραφές, πεδία και στοιχεία. Αυτό όμως το επίπεδο λεπτομέρειας είναι απαγορευτικό για κάποιες εφαρμογές βάσεων δεδομένων. Άλλωστε, μία εγγραφή μπορεί να προσπελαστεί από ένα χρήστη χωρίς αυτό να καταγραφεί, όταν για παράδειγμα εκτελείται μια λειτουργία επιλογής (η προσπέλαση μιας εγγραφής ή ενός πεδίου χωρίς να μεταφέρονται οι πληροφορίες στον χρήστη που τις λαμβάνει καλείται 'πρόβλημα έμμεσης διάσχισης'. Επίσης, είναι δυνατόν να καθοριστούν οι τιμές κάποιων πεδίων χωρίς να προσπελαστούν αυτά άμεσα. Επομένως, η καταγραφή όλων των εγγραφών που έχουν προσπελαστεί από ένα χρήστη άμεσα μπορεί να παρατηρεί αλλά και να μην αποκαλύπτει το μέγεθος αυτών που πραγματικά γνωρίζει.

5.3.2. Έλεγχοι προσπέλασης

Οι βάσεις δεδομένων συνήθως διακρίνονται 'λογικά' από δικαιώματα προσπέλασης χρηστών. Για παράδειγμα, σε όλους τους χρήστες μπορεί να ανατεθούν δικαιώματα προσπέλασης σε γενικά δεδομένα, ενώ μόνο οι θεραπευτές μπορούν να έχουν πληροφορίες για τις θεραπείες και μόνο το οικονομικό προσωπικό μπορεί να έχει πληροφορίες σχετικά με τα έξοδα θεραπείας. Οι βάσεις δεδομένων είναι πολύ χρήσιμες καθώς επικεντρώνουν την αποθήκευση και διατήρηση των πληροφοριών. Η περιορισμένη προσπέλαση είναι συγχρόνως ευθύνη και κέρδος αυτής της συγκέντρωσης.

Ο διαχειριστής της βάσης δεδομένων καθορίζει ποιος επιτρέπεται να προσπελάσει ποιες πληροφορίες, σε επίπεδο πεδίου, ή εγγραφής ή ακόμη και στοιχείου. Το DBMS πρέπει να υποστηρίζει αυτή τη πολιτική, αναθέτοντας δικαιώματα προσπέλασης σε όλες τις συγκεκριμένες πληροφορίες ή ανακλώντας τα όπου επιβάλλεται. Επίσης, οι τύποι της προσπέλασης μπορεί να είναι πολλοί. Ένας χρήστης ή ένα πρόγραμμα μπορεί να έχει το δικαίωμα ανάγνωσης, μεταβολής, διαγραφής ή ενημέρωσης μιας τιμής, προσθήκης ή διαγραφής ολόκληρων πεδίων ή εγγραφών, ή αναδιο-

ργάνωσης όλης της βάσης δεδομένων. Επιφανειακά, ο έλεγχος προσπέλασης μιας βάσης δεδομένων μοιάζει με τον έλεγχο προσπέλασης ενός λειτουργικού συστήματος ή οποιουδήποτε άλλου μέρους ενός πληροφοριακού συστήματος. Εν τούτοις, το πρόβλημα της βάσης είναι πιο περίπλοκο. Τα αντικείμενα ενός λειτουργικού συστήματος, όπως αρχεία, είναι μη συσχετιζόμενα, ενώ οι εγγραφές, τα πεδία και τα στοιχεία μπορούν να συσχετιστούν. Ενώ ένας χρήστης δεν μπορεί να καθορίσει τα περιεχόμενα ενός αρχείου διαβάζοντας άλλα, μπορεί όμως να καταφέρει να προσδιορίσει ένα στοιχείο πληροφορίας διαβάζοντας κάποια άλλα. Το πρόβλημα της εξαγωγής συμπερασμάτων για τις τιμές κάποιων πληροφοριών από κάποιες άλλες καλείται έμμεση προσπέλαση. Είναι δυνατό να προσπελαστούν με έμμεση προσπέλαση, χωρίς να απαιτείται άμεση προσπέλαση στο ίδιο το αντικείμενο που προστατεύεται. Ο περιορισμός των μεσολαβήσεων μπορεί να συνεπάγεται απαγόρευση ορισμένων μονοπατιών, ώστε να αποφεύγονται πιθανές μεσολαβήσεις. Όμως, μπορεί να προκαλέσει και περιορισμό των ερωτημάτων των χρηστών που δεν σκόπευαν να προσπεράσουν τιμές για τις οποίες δεν είναι εξουσιοδοτημένοι. Η πρόσβαση στην βάση δεδομένων μπορεί επίσης να υποβαθμιστεί, ώστε να ελέγχονται οι ζητούμενες παρακλήσεις για πιθανές, ανεπιθύμητες έμμεσες προσπελάσεις.

Τέλος, ο καθορισμός δομικών στοιχείων είναι διαφορετικός για αντικείμενα λειτουργικών συστημάτων και για αντικείμενα βάσεων δεδομένων. Η τήρηση μιας κατάστασης ελέγχου προσπέλασης (access control list) μερικών εκατοντάδων αρχείων είναι πολύ πιο εύκολο να υλοποιηθεί από μια τήρηση κατάστασης ελέγχου προσπέλασης για μια βάση δεδομένων με μερικές εκατοντάδες αρχεία, που ίσως το καθένα από αυτά να αποτελείται επίσης από εκατοντάδες αρχεία. Τα μέγεθος επηρεάζει την αποδοτικότητα της επεξεργασίας.

5.4. Η ΑΝΑΓΚΗ ΓΙΑ ΜΙΑ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΙΑΤΡΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα ιατρικά δεδομένα χαρακτηρίζονται ως ιδιαίτερα ευαίσθητες πληροφορίες των ατόμων στα οποία αναφέρονται. Συνεπώς, κάθε προσπάθεια εισαγωγής πληροφοριακών συστημάτων με Η\Υ για την αποθήκευση και την επεξεργασία τους θα έπρεπε να συνοδεύεται από ικανοποιητικό βαθμό προστασίας από οποιαδήποτε μη εξουσιοδοτημένη χρήση. Η αναγνώριση των διαφόρων τύπων δεδομένων που πιθανώς θα αποθηκευτούν σε τέτοια συστήματα αποτελεί το πρώτο βήμα που γίνεται στην κατεύθυνση της σχεδίασης ασφαλών ιατρικών πληροφοριακών συστημάτων. Συνεπώς, γίνεται και καταγραφή του τρόπου με τον οποίο οι διάφορες κατηγορίες των μελών της ιατρικής κοινότητας αντιμετωπίζουν τη διαβάθμιση των δεδομένων (ως περιορισμένα, εμπιστευτικά, διαθέσιμα στο κοινό) και γενικά την υιοθέτηση μεθόδων, τεχνικών και νομοθεσιών για την παροχή ικανοποιητικών εγγυήσεων ασφάλειας.

Ο σκοπός της κατάστρωσης μιας πολιτικής ασφάλειας για ένα ιατρικό πληροφοριακό σύστημα είναι να αντικατοπτρίσει μια μονόπλευρη άποψη του τρόπου με τον οποίο το ίδρυμα ιατρικής περίθαλψης θα έπρεπε να προσεγγίσει τα σχετικά θέματα και να διαχειριστή την ασφάλεια του. Αυτή η πολιτική προσφέρει ένα οδηγό στις προσδοκίες των ανωτέρων διοικητικών συστημάτων καθώς και ένα σκελετό για δράση και επέκταση.

Ουσιαστικά, η ασφάλεια αποτελεί, σε τελευταία ανάλυση ευθύνη της διοίκησης σε όλα τα επίπεδα. Από τους διοικητές του κάθε επιπέδου ιεραρχίας του ιδρύματος ιατρικής περίθαλψης εξαρτάται η εξασφάλιση της ανάλογης προσοχής και της παροχής των κατάλληλων πόρων στα θέματα ασφάλειας κατά την ανάπτυξη και λειτουργία του πληροφοριακού του συστήματος. Για να εξασφαλίζεται ότι η διαχείριση της ασφάλειας είναι ολοκληρωμένη σε όλο τον οργανισμό, ο κάθε συγκεκριμένος ρόλος πρέπει να έχει στην περιοχή του πλήρη εξουσιοδότηση. Ο όρος πολιτική ασφάλειας θα μπορούσε να περιγραφεί ως εξής: "ποιος μπορεί να κάνει ποιο πράγμα, σε ποια δεδομένα, πότε και από πού". Λαμβάνοντας υπόψη τα ερωτήματα αυτά ο ελεγκτής θα πρέπει να μπορεί να καθορίζει:

Α. Ποιος: όλα τα άτομα που χρησιμοποιούν δεδομένα ή προγράμματα πρέπει να είναι γνωστά και να αναγνωρίζονται θετικά από το σύστημα ελέγχου προσπέλασης τουλάχιστον μέσω ενός συνδυασμού ενός αριθμού χρήστη και ενός συνθηματικού. Άλλες ιδιότητες αναγνώρισης μπορούν να συνδυάσουν κάτι που έχει κάποιος στην κατοχή του με κάτι που γνωρίζει ή κάποιο προσωπικό χαρακτηριστικό (όπως η υπογραφή ή τα δακτυλικά αποτυπώματα).

Β. Ποιο: έπειτα από τη θετική αναγνώριση ακολουθεί ο καθορισμός και η μετάφραση σε δικαιώματα προσπέλασης του:

- τύπου των λειτουργιών που επιτρέπεται στους χρήστες να εκτελούν σε αρχεία δεδομένων
- της κλίμακας των ενεργειών /λειτουργιών και /ή εντολών του Η /Υ που είναι εξουσιοδοτημένοι να χρησιμοποιούν.

Γ. Ποια: όλοι οι χρήστες θα έπρεπε να περιορίζονται στα συγκεκριμένα αρχεία δεδομένων και στη χρήση των ενεργειών/λειτουργιών που έχουν καθοριστεί ως αναγκαίες για την εργασία τους. Αυτή η διαδικασία μπορεί να χρησιμοποιηθεί για να ενισχυθεί ο κατάλληλος καταμερισμός καθηκόντων σε ένα οργανισμό, ελέγχοντας τον τύπο των δεδομένων και τη διαδικασία που ένας οποιοσδήποτε χρήστης είναι εξουσιοδοτημένος να χειρίζεται. Ο καθορισμός της προσεκτικής κατανομής είναι διοικητικό θέμα.

Δ. Πότε: μια πληθώρα ελέγχων που εξαρτώνται από το χρόνο μπορεί να χρησιμοποιηθούν. Για παράδειγμα αυτού του είδους οι έλεγχοι εκτελούνται όταν:

- καθοριστούν οι ώρες της ημέρας που συγκεκριμένες λειτουργίες μπορούν να εκτελεστούν, ή να είναι διαθέσιμα τα δεδομένα ή

- εξασφαλίζεται η αφαίρεση των χαρακτηριστικών αναγνώρισης ή των δικαιωμάτων προσπέλασης χρήστη που έχουν κατανεμηθεί σε προσωρινό ή με σύμβαση προσωπικό μετά τη πάροδο κάποιου χρονικού διαστήματος ή

- καθοριστεί το χρονικό περιθώριο μέσα στο οποίο οι χρήστες οφείλουν να αλλάξουν το συνθηματικό τους ή

- περιοριστεί το χρονικό διάστημα όπου επιτρέπεται ένα τερματικό να βρίσκεται στο σύστημα χωρίς να έχει πιεστεί κανένα πλήκτρο και καθοριστεί αυτόματα πότε το τερματικό θα αποσυνδεθεί από το σύστημα. (εδώ πρέπει να τονίσουμε ότι αυτό είναι διαφορετικό από το 'σβήσιμο' της οθόνης που είναι κάποιες φορές καθορισμένο από τον κατασκευαστή για την αποφυγή εξαντλητικής χρήσης της οθόνης).

Ε. Που: στην περίπτωση αυτή οι έλεγχοι χρησιμοποιούνται για να εξασφαλιστεί ότι συγκεκριμένες λειτουργίες του υπολογιστή μπορούν να εκτελεστούν μόνο σε συγκεκριμένα μέρη. Για παράδειγμα, η δράση του χρήστη θα έπρεπε να περιορίζεται, ώστε να εκτελείται μόνο σε συγκεκριμένα ασφαλή τερματικά.

ΚΕΦΑΛΑΙΟ ΕΚΤΟ

Ασφάλεια Διακίνησης Ιατρικής Πληροφορίας Μέσω Δικτύων.

Περίληψη 6ου κεφαλαίου.

Είναι σαφές ότι σε ένα νοσοκομείο υπάρχουν δεδομένα που είναι *ευαίσθητα* ως προς το περιεχόμενο τους (ιατρικές διαγνώσεις, οικονομικά στοιχεία, εργαστηριακές εξετάσεις).

Γι΄ αυτό το λόγο τα νοσοκομειακά πληροφοριακά συστήματα πρέπει να διαθέτουν υψηλού επιπέδου ασφάλεια και ελέγχου για να αποφεύγονται οι αρνητικές επιπτώσεις που μπορούν να βλάψουν τόσο το νοσοκομείο όσο και τους ασθενείς που νοσηλεύονται σε αυτό. Στο κεφάλαιο αυτό αναφέρονται **οι επιπτώσεις**, που προκύπτουν από την έλλειψη ασφάλειας και ελέγχου, στις διάφορες κατηγορίες εργασιών και υπηρεσιών που λαμβάνουν χώρα σε ένα νοσοκομείο.

6.1. Δημόσια δίκτυα Ο.Τ.Ε.

6.1.1. HELLASPAC:

Η ραγδαία εξέλιξη της πληροφορικής και η ευρύτητα των εφαρμογών της, σε συνδυασμό με τις αυξημένες απαιτήσεις των χρηστών για υψηλού επιπέδου επικοινωνίες δεδομένων είχε σαν αποτέλεσμα τη δημιουργία του **HELLASPAC** από τον Ο.Τ.Ε.

Το HELLASPAC είναι ένα δημόσιο δίκτυο του Ο.Τ.Ε. που είναι άρτια σχεδιασμένο και διαθέτει εξοπλισμό προηγμένης τεχνολογίας για επικοινωνίες δεδομένων μεταξύ των ηλεκτρονικών υπολογιστών και των τερματικών διατάξεων τους. Σ'αυτό το δίκτυο μπορούν να συνδεθούν χρήστες από ολόκληρη την Ελλάδα και μέσω των διεθνών διασυνδέσεων του Ο.Τ.Ε. οι χρήστες μπορούν να συνδεθούν με δίκτυα δεδομένων άλλων χωρών.

Το δίκτυο αυτό είναι ευέλικτο διότι έχει τη δυνατότητα επικοινωνίας μεταξύ τερματικών διαφορετικού τύπου και διαφορετικών ταχυτήτων.

Επίσης παρέχει αξιοπιστία και υψηλής ποιότητας επικοινωνία γιατί λειτουργεί σύμφωνα με τα διεθνή πρότυπα και τις προδιαγραφές που καθορίζει η Διεθνής Ένωση Τηλεπικοινωνιών (I.T.U.).

ΤΟΜΕΙΣ ΠΟΥ ΑΠΕΥΘΥΝΕΤΑΙ

Όπως είδαμε το δίκτυο HELLASPAC μπορεί να καλύψει ανάγκες για μεταβίβαση, άντληση ή αποθήκευση σε όλους τους τομείς εφαρμογών της πληροφορικής μεταξύ άλλων και στον Ιατρικό τομέα.

6.1.2. Τα πλεονεκτήματά του.

Ο Ο.Τ.Ε. σχεδιάζοντας το HELLASPAC, ανταποκρίθηκε στις σημερινές ανάγκες των χρηστών στην Ελλάδα για υψηλού επιπέδου επικοινωνίες δεδομένων, προσφέροντας μια σειρά από σημαντικά πλεονεκτήματα:

Αξιοπιστία: γιατί το δίκτυο χρησιμοποιεί εξοπλισμούς προηγμένης τεχνολογίας και διαθέτει για όλες τις σημαντικές εγκαταστάσεις αντίστοιχες εφεδρικές που βρίσκονται πάντα σε ετοιμότητα για εναλλακτική δρομολόγηση της μεταβιβαζόμενης κίνησης σε περίπτωση βλάβης.

Ευελιξία: γιατί παρέχει στο χρήστη την ευχέρεια επιλογής της βασικής υπηρεσίας και των ευκολιών εκείνων που εξυπηρετούν τις συγκεκριμένες εφαρμογές του. Επίσης κάνει εφικτή την επικοινωνία μεταξύ των τερματικών εξοπλισμών διαφορετικού τύπου και διαφορετικών ταχυτήτων.

Ποιότητα επικοινωνίας: γιατί η τεχνική που υιοθετήθηκε εξασφαλίζει υψηλή προστασία από σφάλματα που μπορεί να προκύψουν κατά τη διάρκεια ανταλλαγής πληροφοριών.

Τυποποίηση: λειτουργεί σύμφωνα με τα διεθνή πρότυπα και τις προδιαγραφές που καθορίζει η Διεθνή Ένωση Τηλεπικοινωνιών (I.T.U.).

Ασφάλεια: γιατί η χρησιμοποιούμενη τεχνική μετάδοσης δεδομένων ελαχιστοποιεί τον κίνδυνο αυθαίρετης παρέμβασης στις επικοινωνίες και παρέχει πρόσθετη ασφάλεια και προστασία στους χρήστες του.

Επεκτασιμότητα: το δίκτυο έχει τη δυνατότητα να επεκτείνει ή να αυξήσει τη χωρητικότητα του ώστε ανάλογα με τη ζήτηση που υπάρχει, να ικανοποιεί μεγαλύτερο αριθμό χρηστών.

6.1.3. Γενική δομή του HELLASPAC

Το δίκτυο HELLASPAC αποτελείται από κόμβους (Κέντρα Μεταγωγής πακέτων Δεδομένων – Κ.Μ.Δ.) που έχουν εγκατασταθεί και λειτουργούν σε διάφορες πόλεις της Ελλάδας. Οι κόμβοι που λειτουργούν σε Αθήνα, Πειραιά, Θεσσαλονίκη, Πάτρα, και Ηράκλειο αποτελούν κέντρα μεγάλης δυναμικότητας και αποτελούν τον κύριο άξονα πάνω στον οποίο δομείται όλο το ΔΙΚΤΥΟ. Τα υπόλοιπα μικρότερα κέντρα στηρίζονται πάνω στα προηγούμενα χωρίς όμως να υστερούν σε ότι αφορά στις παρεχόμενες προς τους συνδρομητές υπηρεσίες και ευκολίες. Στον κόμβο της Αθήνας βρίσκεται ενσωματωμένο το κέντρο Διαχείρισης και Ελέγχου (Network Control and Management – NCMC) το οποίο είναι επιφορτισμένο με σημαντικές αρμοδιότητες για την ορθή και αδιάκοπη λειτουργία του Δικτύου. Είναι υπεύθυνο για τον έλεγχο και τη δρομολόγηση της κίνησης, τη χρέωση των επικοινωνιών, τη στατιστική παρακολούθηση της ποιότητας των προσφερόμενων υπηρεσιών, τη σηματοδοσία των βλαβών και τον έλεγχο της απόδοσης.

6.1.4. Τεχνική μετάδοσης δεδομένων στο HELLASPAC

Το δίκτυο HELLASPAC, για την μετάδοση των δεδομένων χρησιμοποιεί την ***μέθοδο αποθήκευσης και μεταγωγής πακέτων,*** όπου χρησιμοποιούνται σύγχρονοι ψηφιακοί εξοπλισμοί οι οποίοι δρομολογούν τα δεδομένα στον προορισμό τους. Τα δεδομένα που στέλνει κάποιος χρήστης στο δίκτυο διασπώνται σε πλαίσια δεδομένων ορισμένου μεγέθους όπου σε κάθε τμήμα

εισάγει στοιχεία για τον έλεγχο τυχόν λανθασμένων μεταβιβάσεων. Επίσης εισάγει πληροφορίες απαραίτητες για την δρομολόγηση του μηνύματος στον παραλήπτη όπως διεύθυνση προορισμού, ταυτότητα αποστολέα. Όλα αυτά γίνονται με μια τεχνική διάταξη που μπορεί να βρίσκεται στις εγκαταστάσεις του χρήστη ή στο δίκτυο.

Το δίκτυο, περιλαμβάνει ορισμένο αριθμό κέντρων μεταγωγής πακέτων που συνδέονται μεταξύ τους με κυκλώματα μεγάλων ταχυτήτων. Κάθε κέντρο μεταγωγής αναγνωρίζει τη διεύθυνση προορισμού των πακέτων και τα κατευθύνει κατάλληλα μέχρι να φθάσουν στο σημείο προορισμού. Εκεί αφαιρούνται οι υπηρεσιακές πληροφορίες που συνοδεύουν κάθε πακέτο και το μήνυμα παίρνει την αρχική του μορφή. Επειδή κάθε πακέτο περιέχει την δική του διεύθυνση προορισμού και τις δικές του υπηρεσιακές ενδείξεις κάνει δυνατή την ταυτόχρονη μεταβίβαση δεδομένων σε διαφορετικούς χρήστες. Αυτό έχει σαν αποτέλεσμα να βελτιώνεται η απόδοση των μέσων μετάδοσης του δικτύου και να μειώνεται το κόστος χρήσης του. Έτσι, το δίκτυο θεωρείται από τον χρήστη σαν μέσο μετάδοσης όπου στέλνει τα μηνύματα του ορίζοντας μόνο την διεύθυνση προορισμού και από εκεί και πέρα το δίκτυο αναλαμβάνει να τα μεταδώσει γρήγορα και με ασφάλεια στον προορισμό τους.

6.1.5. Τεχνικός εξοπλισμός

Ο υποψήφιος χρήστης του HELLASPAC για να συνδεθεί στο δίκτυο πρέπει να διαθέτει κατάλληλο τεχνικό εξοπλισμό στο χώρο του. Ο εξοπλισμός αυτός που αποτελεί το σταθμό δεδομένων χρήστη, περιλαμβάνει:

- τη Συσκευή Τερματισμού Κυκλώματος δεδομένων π.χ. MODEM (διαποδιαμορφωτή)
- τη Τερματική Συσκευή Δεδομένων π.χ. Η\Υ, τερματικό
- τον εξοπλισμό παρεμβάλλεται μεταξύ τους.

6.1.6. Κυριότερες ευκολίες του HELLASPAC

Παρακάτω θα γίνει μια αναφορά στις κυριότερες ευκολίες που προσφέρει το δίκτυο:

1. Κλειστή ομάδα χρηστών: Εδώ επιτρέπεται σε μια ομάδα χρηστών, να επικοινωνούν μεταξύ τους (κλειστή ομάδα) αποκλειόμενης κάθε εισερχόμενης ή εξερχόμενης κλήσης προς ή από τα μέλη της ομάδας. Επίσης παρέχεται ένας πρόσθετος βαθμός ασφάλειας, αφού κανένας ανεπιθύμητος δεν μπορεί να επικοινωνήσει με κάποιον από την ομάδα, αλλά και κανένα μέλος της ομάδας δεν μπορεί να επικοινωνήσει με συνδρομητή του δικτύου. Η ευκολία αυτή μπορεί να προσφερθεί με διάφορες παραλλαγές όπως:

Α) ***Κλειστή ομάδα χρηστών με δυνατότητα εξερχόμενων κλήσεων:*** πραγματοποιούνται εξερχόμενες κλήσεις προς άλλους χρήστες που δεν ανήκουν στην ομάδα.

Β) Κλειστή ομάδα χρηστών με δυνατότητα εισερχόμενων κλήσεων:

Μέλη της ομάδας δέχονται εισερχόμενες κλήσεις από άλλους χρήστες εκτός ομάδας.

Γ) ***Φραγή εξερχόμενων κλήσεων μέσα σε κλειστή ομάδα χρηστών:*** απαγόρευση πραγματοποίησης κλήσης από τα μέλη μιας ομάδας προς τα μέλη της ίδιας ομάδας. Επίσης έχει εφαρμογή σε όλα τα λογικά κανάλια της σύνδεσης.

Δ) ***Φραγή εισερχόμενων κλήσεων μέσα σε κλειστή ομάδα χρηστών:*** απαγόρευση στην ομάδα να δέχεται κλήσεις από άλλα μέλη της ίδιας ομάδας. Επίσης έχει εφαρμογή σε όλα τα λογικά κανάλια της σύνδεσης.

2. ***Επιλογή κλειστής ομάδας χρηστών ανά κλήση.*** Σε περίπτωση που κάποιος χρήστης ανήκει σε περισσότερες από μια κλειστές ομάδες επιλέγει σε κάθε κλήση τη συγκεκριμένη ομάδα με την οποία επιθυμεί να επικοινωνήσει.

3. ***Λογικό κανάλι με προκαθορισμένο χρήστη.*** Παρέχεται η δυνατότητα προγραμματισμού ενός ή περισσοτέρων λογικών καναλιών να βλέπουν πάντοτε το ίδιο τερματικό από την άλλη πλευρά.

4. ***Μη τυποποιημένο μέγεθος πακέτο.*** Ο χρήστης έχει τη δυνατότητα επιλογής του μεγέθους των πακέτων των επικοινωνιών του με ανώτατο όριο τα 256 bytes. Σε περίπτωση που δεν έχει ζητηθεί η ευκολία αυτή τότε το δίκτυο εισάγει το τυποποιημένο μέγεθος πακέτου δηλαδή 128 bytes.

5. ***Διαπραγμάτευση του ρυθμού μετάδοσης πληροφορίας.*** Ο χρήστης μπορεί να διαπραγματεύεται ανά κλήση το ρυθμό μετάδοσης πληροφορίας και να τον μεταβάλλει αλλά ο ρυθμός αυτός θα είναι πάντα μικρότερος από τον αρχικό ζητούμενο στην αρχική αίτηση του.

6.2. HELLASCOM

Γενικά

Το δίκτυο HELLASCOM είναι ένα εθνικό, τηλεπικοινωνιακό δίκτυο μετάδοσης δεδομένων και φωνής. Είναι ειδικά σχεδιασμένο βάσει διεθνών προδιαγραφών και παρέχει μισθωμένα, ψηφιακά, σταθεροζευκτικά κυκλώματα χαμηλής ή υψηλής ταχύτητας, σε χρήστες που βρίσκονται σε οποιοδήποτε μέρος της χώρας.

Το δίκτυο έχει τη δυνατότητα αμφίδρομης επικοινωνίας από σημείο σε σημείο και από σημείο προς πολλαπλά σημεία για συνεχή χρήση. Υλοποιείται

με την χρήση κόμβων και τερματικών μονάδων δικτύου, που ελέγχονται από το κέντρο διαχείρισης και ελέγχου. Έτσι είναι δυνατός ο έλεγχος της διασύνδεσης του συνδρομητή από άκρο σε άκρο, ώστε να ανιχνευτεί οποιαδήποτε δυσλειτουργία του κυκλώματος και να επέμβει με σκοπό την αποκατάστασή της.

6.2.1. Τομείς που απευθύνεται.

Το δίκτυο HELLASCOM απευθύνεται σε χρήστες που ζητούν ανταλλαγή μεγάλου όγκου πληροφοριών και υψηλή ποιότητας μετάδοσης με ευελιξία, αξιοπιστία, ασφάλεια και οικονομία. Απευθύνεται κυρίως σε:

- Μεγάλες Επιχειρήσεις και Οργανισμούς του Ιδιωτικού και Δημοσίου τομέα όπως τράπεζες, βιομηχανίες, ασφαλιστικές εταιρείες.
- Μεγάλα Νοσοκομεία (εφαρμογές Τηλεϊατρικής).
- Εκπαιδευτικά Ιδρύματα.
- Εταιρίες Τηλεπικοινωνιών, Πληροφορικής.

6.2.2. Κέντρο διαχείρισης και ελέγχου.

Ο εξοπλισμός της ψηφιακής διασύνδεσης και οι ευέλικτοι πολυπλέκτες ελέγχονται από το κέντρο διαχείρισης και ελέγχου δικτύου, το οποίο ορίζει την διάρθρωση και την παρακολούθηση της λειτουργικής κατάστασης του δικτύου. Η πληροφορία, που ανταλλάσσεται ανάμεσα στο κέντρο διαχειρίσης και ελέγχου δικτύου και με οποιοδήποτε άλλο εξοπλισμό, γίνεται πάνω στο δίκτυο μεταγωγής πακέτων με πρωτόκολλο Χ.25. Η όλη λειτουργία του HELLASCOM ελέγχεται από το Κέντρο Διαχείρισης και Ελέγχου που παρέχει σε όλη του την έκταση κεντρικά συντονισμένη διαχείριση και έλεγχο. Το κέντρο διαχείρισης και ελέγχου επιτρέπει:

- Την αυτόματη δρομολόγηση ή αναδρομολόγηση κυκλωμάτων data αρίστης ποιότητας με υψηλές ταχύτητες.
- Την διαχείριση και τον έλεγχο του δικτύου μέχρι το χρήστη.
- Τη διαχείριση τμήματος του δικτύου από τον ίδιο τον χρήστη εφόσον προηγηθεί συμφωνία με τον Ο.Τ.Ε.
- Την καταγραφή πληροφοριών για τη διαθεσιμότητα των γραμμών και της χρησιμοποίησης τους για λόγους χρέωσης.

6.2.2.1. Σύνθεση του κέντρου ελέγχου και διαχείρισης

Το N.M.S. υλοποιείται μέσω ενός δικτύου υπολογιστών βάσει της σύστασης CCITT M.3010. Τα επιμέρους στοιχεία του δικτύου επικοινωνούν με το N.M.S. μέσω του πρωτοκόλλου X.25. Οι πληροφορίες μεταδίδονται μέσω ενός καναλιού που ονομάζεται E.O.C. (EMBEDED OPERATION CHANNEL) και ρέουν μέσω των ίδιων φορέων του δικτύου. Το κέντρο διαχείρισης και ελέγχου αποτελείται από τα παρακάτω επί μέρους στοιχεία:

Δύο ηλεκτρονικούς υπολογιστές (ένα κύριο και ένα εφεδρικό) τύπου DEC VAX της DIGITAL.Μια σειρά από τερματικά για τους χειριστές του συστήματος.Ένα δίκτυο τύπου Ethernet, που συνδέει τους υπολογιστές με τα τερματικά.
Τρεις δρομολογητές, που οδηγούν τα κανάλια E.O.C. όλων των κόμβων σε λογικά κανάλια κατά το πρωτόκολλο X.25.

Ένα κόμβο πρόσβασης στον οποίο οδηγούνται τα προαναφερθέντα κανάλια και από εκεί δρομολογούνται στο πλησιέστερο D.X.C. για να συνεχίσουν την πορεία τους μέχρι το τελικό προορισμό τους, δηλαδή τους κόμβους, που θα τα χειριστούν.

6.2.2.2. Έλεγχος των λειτουργικών μονάδων

Το κέντρο ελέγχου και διαχείρισης επιτελεί ένα πλήθος σημαντικών λειτουργιών, ελέγχει όλες τις λειτουργικές μονάδες του και πιο συγκεκριμένα:

- Ενεργοποιεί / Απενεργοποιεί τις λειτουργικές μονάδες.
- Πραγματοποιεί / Διακόπτει τις συνδέσεις.
- Ενεργοποιεί τους βρόχους μέσω λογισμικού.
- Ρυθμίζει παραμέτρους λειτουργίας των κόμβων.
- Διαμορφώνει την τοπολογία του δικτύου προσθέτοντας, καταργώντας ή τροποποιώντας τις ζεύξεις που συνθέτουν το δίκτυο.
- Διαχειρίζεται σηματοδοσίες (μεταβολές στην κατάσταση των λειτουργικών μονάδων, υπερβάσεις ορίων ποιότητας, κακή λειτουργία του SOFTWARE- HARDWARE στο NMS, εντοπίζει τη μονάδα που προκάλεσε τη σηματοδοσία).
- Ενεργοποιεί αυτοδιαγνωστικά προγράμματα .
- Πραγματοποιεί εξειδικευμένες μετρήσεις (χρονικό διάστημα που δεν είναι διαθέσιμο το κύκλωμα, δευτερόλεπτα που μεταδίδονται λανθασμένα, λεπτά υποβαθμισμένης λειτουργίας).
- Συλλέγει και επεξεργάζεται στατιστικά στοιχεία (στοιχεία πρόσβασης, χρήστες, διάρκεια εκμετάλλευσης των κυκλωμάτων, κατάσταση και διαμόρφωση κάθε μονάδας, χρεώσεις, στοιχεία ποιότητας).

6.3. Ιδιωτικά δίκτυα δεδομένων.

Τα ιδιωτικά δίκτυα δεδομένων (PRIVATE NETWORK- PN) υλοποιούνται με την ενοικίαση μόνιμων αφιερωμένων κυκλωμάτων ή με τη χρήση ιδιωτικών γραμμών ζεύξης. Το κύκλωμα μπορεί να είναι δισύρματο ή τετρασύρματο συνεστραμμένο ζεύγος καλωδίων, ομοαξονικό καλώδιο, μικροκυματική ζεύξη, οπτική ίνα, δορυφορική ζεύξη. Συνήθως ο οργανισμός τοποθετεί ιδιωτικά συστήματα έξυπνης πολύπλεξης (IMUX- INTELLIGENT MULTIPLEXERS) τα οποία έχουν τη δυνατότητα να μεταφέρουν δεδομένα αλλά και φωνή. Η ασφάλεια των δεδομένων (μια και η ζεύξη είναι αποκλειστική) είναι ανάμεσα στα θετικά των ιδιωτικών δικτύων. Επιπλέον, ο οργανισμός μπορεί να επιλέξει ο ίδιος τα πρωτόκολλα που θα τρέξει στα νοικιασμένα κυκλώματα έχοντας έτσι τη μεγαλύτερη δυνατή ευελιξία. Το μειονέκτημα των ιδιωτικών δικτύων δεδομένων είναι το μεγάλο κόστος των κυκλωμάτων (αυξάνει ανάλογα με την ταχύτητα) καθώς και το κόστος εγκατάστασης των συστημάτων μεταγωγής. Στην πράξη μόνο μεγάλοι οργανισμοί και επιχειρήσεις μπορούν να ανεχθούν το υψηλό κόστος λειτουργίας ενός ιδιωτικού δικτύου δεδομένων, αλλά και να διακινούν δεδομένα ολόκληρο το 24ωρο, ώστε να έχουν μέγιστη εκμετάλλευση του δικτύου. Σε γενικές γραμμές το κόστος του κυκλώματος είναι ανάλογο της ταχύτητας και της απόστασης. Τις περισσότερες φορές τα κυκλώματα αποτελούνται είτε από χάλκινους αγωγούς είτε από συνδέσεις οπτικών ινών. Στην περίπτωση που η απόσταση μεταξύ των κόμβων που θα διασυνδεθούν είναι μεγάλη, συμφέρει η ενοικίαση δορυφορικών υπηρεσιών.

6.4. Επικοινωνία με άλλους φορείς.

6.4.1. Η χρήση της κρυπτογραφίας για την ασφαλή ανταλλαγή πληροφοριών – δεδομένων.

6.4.1.1. Ασφαλής προσπέλαση

Η σύνδεση ενός χρήστη σε ένα δίκτυο υπολογιστών επιτυγχάνεται με την τεχνική των συνθηματικών (passwords). Είναι γνωστό ότι η τεχνική αυτή δεν είναι ασφαλής και παρουσιάζει πλήθος προβλημάτων. Για παράδειγμα, το συνθηματικό μπορεί να αποκαλυφθεί κατά την πληκτρολόγηση του σε ένα παρευρισκόμενο. Ακόμη η σύνδεση σε ένα απομακρυσμένο υπολογιστή εκθέτει το χρήστη σε υποκλοπές του συνθηματικού. Επειδή η επιλογή των συνθηματικών είναι συνήθως περιορισμένη, η εύρεση τους από τρίτους μπορεί να επιτευχθεί εύκολα χωρίς ιδιαίτερη παραβίαση του συστήματος. Γενικότερα, στο πρόβλημα της ασφαλούς σύνδεσης εμπίπτουν οι περιπτώσεις των ηλεκτρονικών καρτών των Νοσοκομείων, των τραπεζικών μηχανημάτων κ.α. Μια ασφαλής προσπέλαση μπορεί να επιτευχθεί με τη χρήση κρυπτογραφικών τεχνικών. Μια τέτοια τεχνική βασίζεται σε μια διαδικασία κλήσης – απόκρισης των εμπλεκόμενων μερών και χρησιμοποιεί ψηφιακές υπογραφές. Σε αυτήν ο χρήστης υπογράφει μια τυχαία συμβολοσειρά του συστήματος η οποία επαληθεύεται από το σύστημα. Μια άλλη

τεχνική βασίζεται σε συστήματα μηδενικής γνώσης. Σε αυτή τη τεχνική ο χρήστης εφοδιάζεται με μια υπογραφή της ταυτότητάς του από ένα αρμόδιο κέντρο. Κατά την πραγματοποίηση μιας προσπέλασης χρησιμοποιεί ένα σύστημα μηδενικής γνώσης για να αποδείξει ότι γνωρίζει την υπογραφή χωρίς να την αποκαλύψει. Η υλοποίηση και των δυο αυτών τεχνικών μπορεί να γίνει με τη χρήση έξυπνων καρτών.

6.4.1.2. Ψηφιακά διαβατήρια

Τα διαβατήρια είναι ένας τρόπος αναγνώρισης ταυτότητας. Με τη χρήση των ηλεκτρονικών υπογραφών είναι δυνατό να δημιουργηθούν ασφαλή ψηφιακά διαβατήρια. Η τεχνική είναι ανάλογη με αυτή της ασφαλούς προσπέλασης. Κάθε κράτος εκδίδει ένα ψηφιακό διαβατήριο το οποίο περιλαμβάνει μια υπογραφή της ταυτότητας του χρήστη. Έτσι, όταν ο κάτοχος του διαβατηρίου θέλει να ταυτοποιηθεί αποδεικνύει, χρησιμοποιώντας ένα πρωτόκολλο μηδενικής γνώσης, ότι γνωρίζει την υπογραφή χωρίς να την επιδείξει. Επειδή η αποκάλυψη της αποδείξεως μπορεί να οδηγήσει σε πλαστογράφηση είναι απαραίτητο το ψηφιακό διαβατήριο να υλοποιηθεί με tamper-free συσκευές όπως οι έξυπνες κάρτες.

6.4.1.3. Ηλεκτρονική μεταβίβαση δεδομένων

Η ηλεκτρονική μεταβίβαση δεδομένων E.D.I. (Electronic Data Interchange) είναι μια τεχνική ηλεκτρονικής μεταφοράς μηνυμάτων μεταξύ πληροφοριακών συστημάτων σύμφωνα με καθορισμένα πρότυπα δόμησης. Στις ανεπτυγμένες εμπορικά χώρες η τεχνική αυτή αποτελεί καθημερινή πρακτική για την διεκπεραίωση διαφόρων συναλλαγών, αποφεύγοντας το συμβατικό τρόπο επεξεργασίας και ανταλλαγής εγγράφων. Σύμφωνα με αυτή οι ανταλλασόμενες εντολές μορφοποιούνται με αυστηρά καθορισμένα πρότυπα έτσι ώστε να αναγνωρίζονται από τα υπολογιστικά συστήματα των εμπλεκομένων μερών. Η όλη διαδικασία ολοκληρώνεται εντός ελαχίστου χρόνου ηλεκτρονικά. Για την γνησιότητα και ακεραιότητα μιας εντολής, στα πλαίσια του E.D.I., μπορεί να χρησιμοποιηθεί η τεχνική της ψηφιακής υπογραφής, ενώ η εξασφάλιση της μυστικότητας των ανταλλασόμενων εντολών επιτυγχάνεται με τη χρήση κρυπτογραφικών τεχνικών. Η παρεχόμενη ασφάλεια εξαρτάται από το χρησιμοποιούμενο κρυπτογραφικό σύστημα.

6.5. Συστήματα Υπηρεσίας Πληροφοριών Υγείας

Κάθε πλευρά του συστήματος ιατρικής περίθαλψης παρουσιάζει τις δικές του ιδιαίτερες προκλήσεις. Έχει συμφωνηθεί μεταξύ αρκετών, ότι η αποδέσμευση επίκαιρων ασφαλιστικών πληροφοριών είναι πολύ λιγότερο εμπιστευτική από την αποδέσμευση παθολογικών εξετάσεων. Σύμφωνα με την ομόφωνη γνώμη αμερόληπτων παραγόντων ασφάλειας, η πρόσβαση των

γιατρών σε ιατρικές πληροφορίες ασθενών θα πρέπει να είναι λιγότερο περιοριστική από αυτή του προσωπικού της κλινικής. Στην περίπτωση των πληροφοριών που αφορούν ασθενείς, η υιοθέτηση λογικής σκέψης φαίνεται ότι είναι μία αποδεκτή διαδικασία και έτσι, οι περισσότεροι κανόνες που διέπουν τα *ηλεκτρονικά* ιατρικά δεδομένα έχουν διαμορφωθεί έπειτα από μακροχρόνιες διαδικασίες. Η πρόσβαση στους ηλεκτρονικούς υπολογιστές παραλληλίζεται με τη χρήση των έντυπων διαγραμμάτων.

"Αυτό δεν είναι δυνατόν!! Όλοι γνωρίζουν ότι η γραφειοκρατική διαδικασία είναι ανεπαρκής. Θα πρέπει να εξασφαλίσουμε την αποφυγή διαρροών και την ασφάλιση το συστήματος." Σε αυτό το σημείο η λογική διαδικασία μετατρέπεται σε παράνοια ασφάλειας ... πλήρως τεκμηριωμένη, χωρίς όμως αναγνώριση του γεγονότος ότι η ηλεκτρονική ασφάλεια είναι εξίσου ευάλωτη στην καταστρατήγηση όσο και η γραφειοκρατική. Επίσης η υπηρεσία Πληροφοριών αδυνατεί να ανταποκριθεί στις συνεχώς αυξανόμενες απαιτήσεις για περισσότερη ασφάλεια στο σύστημα και στην τήρηση του απορρήτου για τις πληροφορίες των ασθενών.

Ακόμα, η Υπηρεσία Πληροφοριών (I.S.) προσφέρει λειτουργική και αναπτυξιακή υποστήριξη σε απεριόριστο αριθμό ιατρικών πρωτοβουλιών και είναι πλέον εμφανές ότι η Ουτοπία, όπως πάντα, δεν αποτελεί επιλογή. Η καλύτερη προσέγγιση είναι η καταβολή ενσυνείδητης προσπάθειας για τη δημιουργία *ισορροπημένης* ασφάλειας μεταξύ των κοινωνικών προβληματισμών και της πρόσβασης του νοσηλευτικού προσωπικού.

Στην προσπάθεια δημιουργίας Μηχανογραφημένου Αρχείου Ασθενών (C.P.R.), σε διάφορα συστήματα υγείας ενσωματώθηκαν βασικές αρχές ακρίβειας δεδομένων, απόρρητου και ασφάλειας, οι οποίες βρίσκουν εφαρμογές σε θέματα ηλεκτρονικής αποθήκευσης και παρουσίασης ιατρικών πληροφοριών. Αυτά τα μέτρα αποτελούν σήμερα αναπόσπαστο μέρος οποιασδήποτε παρόμοιας πρωτοβουλίας. Όπως είπαμε και στις προηγούμενες παραγράφους, αυτές οι βασικές αρχές συνεχίζουν να ισχύουν έπειτα από ανάπτυξη και χρήση οκτώ ετών. Δεν έχουν απειληθεί από κανένα νομικό ελιγμό. Παρέχουν μέγιστη πρόσβαση στα απαραίτητα ιατρικά δεδομένα και ελαχιστοποιούν τον κίνδυνο παραβίασης του απόρρητου του ασθενή. Η ανάπτυξη της αγοράς μπορεί να επιβάλλει μεταβολές για την εξυπηρέτηση ενός ευρύτερου κοινού ... αλλά, αυτά τα στοιχεία, με την απλότητά και την κοινή λογική που τα διέπουν, αποτελούν έντιμες προσπάθειες καθιέρωσης και διατήρησης της ισορροπίας μεταξύ της νομικής υποχρέωσης και της υπερβολικής ασφάλειας.

Το γεγονός ότι το βασικό μας προϊόν είναι η ολοκληρωμένη, ποιοτική περίθαλψη υπερκαλύπτει όλα τα άλλα στοιχεία και καθώς είμαστε επαγγελματίες, θα πρέπει να χρησιμοποιήσουμε οποιοδήποτε διαθέσιμο ηλεκτρονικό βοήθημα για την επίτευξη του σκοπού μας.

6.5.1. Ιστορικό

Παράδειγμα

Το Σύστημα Διαχείρισης Ιατρικών Πληροφοριών (M.I.M.S.) του Συστήματος Υγείας Henry Ford, επιτρέπει πρόσβαση πραγματικού χρόνου (real time) σε ιατρικά δεδομένα ασθενών, 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα. Η πρόσβαση στη βάση δεδομένων των 270 εκατομμυρίων μητρώων είναι δυνατή από άνω των 60 κέντρων περίθαλψης τα οποία βρίσκονται εντός

ακτίνας 120 μιλίων του Μητροπολιτικού Ντιτρόιτ. Το σύστημα μηχανογράφησης ασθενών είναι ακόμα προσβάσιμο από ομάδες γιατρών από θέσεις εκτός δικτύου. Μεταξύ των πελατών του συστήματος συμπεριλαμβάνονται γιατροί, νοσοκόμες, ιατρικοί βοηθοί, τεχνικοί, θεραπευτικό προσωπικό, προσωπικό ιατρικού αρχείου και διάφοροι άλλοι υπάλληλοι του οικονομικού κλάδου του Συστήματος Υγείας.

Από τότε που τέθηκε σε λειτουργία, εδώ και πάνω από οκτώ χρόνια, το M.I.M.S. προσπαθεί να τηρήσει λεπτές ισορροπίες μεταξύ της επαρκούς προστασίας του απόρρητου των δεδομένων των ασθενών και της επαρκούς πρόσβασης στα δεδομένα από το νοσηλευτικό προσωπικό, παρέχοντας έτσι την καλύτερη δυνατή ποιότητα περίθαλψης, εκπαίδευση και έρευνα. Οι τακτικές και οι διαδικασίες που έχουν προκύψει, αν και δεν είναι τέλειες, εξυπηρετούν αυτή τη διχοτόμηση.

Κανείς δεν μπορεί να αμφισβητήσει την εκπληκτική πρόοδο που έχει επιτύχει η βιομηχανία των ηλεκτρονικών υπολογιστών στον τομέα συγκέντρωσης δεδομένων. Ο γενικός πληθυσμός έχει υποστεί πολλά μικροατυχήματα, τα οποία οφείλονται σε ατελή μηχανογραφικά συστήματα τα οποία χρεώνουν εσφαλμένα, παρακολουθούν παράνομα και είναι υπεύθυνα για τη δημιουργία μεγάλων καταλόγων αποστολής διαφημιστικών εντύπων. Το βάρος αντιμετώπισης της προκατάληψης που έχουν δημιουργήσει αυτά τα συστήματα, αλλά και η εξάλειψη του φόβου παραβίασης του απόρρητου των ασθενών, έχει πέσει στους επαγγελματίες της πληροφορικής στο χώρο της περίθαλψης. Για την ανάπτυξη ενός περιβάλλοντος εμπιστευτικότητας δεδομένων και ασφάλειας, η Συμβουλευτική Επιτροπή του M.I.M.S. κατά το σχηματισμό της αρχικής πλατφόρμας ασφάλειας της, προσδιόρισε τέσσερις μεγάλες κατηγορίες. Τον **Ασθενή**, τον **Πελάτη**, τη **Βάση Δεδομένων** και την **Ευθύνη**, η οποία σχετίζεται με όλες τις προηγούμενες τρεις κατηγορίες.

6.5.2. Ο Ασθενής

Καθώς η τεχνολογία των ηλεκτρονικών υπολογιστών παρέχει μεγαλύτερη δυνατότητα πρόσβασης σε δεδομένα ασθενών από ότι τα έντυπα διαγράμματα, κρίθηκε αναγκαία η επίδειξη περισσότερης προσοχής σε θέματα ασφάλειας όσον αφορά τα αρχεία δεδομένων και την συνεπακόλουθη πρόσβασή τους.

Το πρώτο βήμα σε αυτή τη διαδικασία ήταν η καθιέρωση και προτοποθέτηση στο βασικό πίνακα κάθε ασθενή, ενός ειδικού δείκτη ο οποίος κατατάσσει τον ασθενή σε μία κατηγορία. Δημιουργήθηκαν τρεις κατηγορίες ασθενών. Ο ασθενής του Συστήματος Υγείας, ο Υπάλληλος ασθενής και ο Επίσημος ασθενής V.I.P. (Very Important Person).

6.5.3. Ο ασθενής του συστήματος υγείας

Ορίζοντας απλά τον ασθενή του Συστήματος Υγείας, θα λέγαμε ότι είναι οποιοδήποτε εσωτερικός ή εξωτερικός ασθενής νοσοκομείου, σε οποιοδήποτε επίπεδο του οργανισμού. Τα έντυπα αρχεία για αυτή την κατηγορία ασθενών συμπληρώνονται στο Τμήμα Ιατρικών Αρχείων χωρίς εξαιρέσεις. Η

ηλεκτρονική εκπροσώπηση των δεδομένων των πινάκων αποτελούν νόμιμα μέρος του αρχείου δεδομένων του M.I.M.S. και βασίζεται στην κατηγορία του κωδικού του ασθενή.

6.5.4. Ο υπάλληλος ασθενής

Κάθε υπάλληλος ή μελλοντικός υπάλληλος υποβάλλεται σε προκαταρκτικές εξετάσεις στις εγκαταστάσεις του Συστήματος Υγείας και συνεπώς, γίνεται αυτομάτως "ασθενής του Συστήματος Υγείας". Η Επιτροπή του MIMS, καθώς αποτελεί τον όγδοο μεγαλύτερο εργοδότη της Πολιτείας του Μίτσιγκαν και αναγνωρίζοντας την υποβόσκουσα περιέργεια των συνεργατών, αναγνώρισε την ανάγκη προσθήκης ενός ακόμα επιπέδου ασφάλειας σε ασθενείς οι οποίο ήταν υπάλληλοι.

Καθιερώθηκαν και μπήκαν σε εφαρμογή διαδικασίες οι οποίες επιτρέπουν στους υπαλλήλους να υποδεικνύουν το επίπεδο ασφάλειας ανάκλησης των διαθέσιμων μέσω διαδικτύου ηλεκτρονικών αρχείων τους, κατά τη διάρκεια της ιατρικής περίθαλψης τους. Τα επίπεδα αυτά είναι (1) Δεν επιτρέπεται η πρόσβαση, (2) Επιτρέπεται η πρόσβαση μόνο σε γιατρό, ή (3) Γενική πρόσβαση σε πελάτες του M.I.M.S.

Κατά τη διάρκειας μίας μεγάλης έρευνας, ερωτήθηκαν όλοι οι υπάλληλοι να σταθμίσουν τις συνέπειες της περιορισμένης πρόσβασης, π.χ., καταστάσεις τραυματισμού, επισκέψεις για εξετάσεις ... ή περιπτώσεις κατά τις οποίες ο έντυπος ιατρικός πίνακας μπορεί να μην είναι διαθέσιμος. Η ανταπόκριση είχε σαν αποτέλεσμα το 1% των ερωτηθέντων να ζητήσει "τήρηση του απορρήτου" ενώ το υπόλοιπο 99% επέλεξε την "πρόσβαση από το γιατρό". Ακόμα, παρατηρείται μία τάση προς "γενική" πρόσβαση (αιτήσεις υπαλλήλων για "άνοιγμα" των αρχείων τους σε όλους τους χρήστες). Μία προκαταρκτική έρευνα χρεώνει αυτή την παραδειγματική μετατόπιση στον πολλαπλασιασμό των παραϊατρικών (όχι γιατρών) νοσηλευτών, καθώς και στο ιστορικό αξιοπιστίας και ακρίβειας της βάσης δεδομένων του MIMS.

Σήμερα, η επιλογή του υπαλλήλου αποτελεί αναπόσπαστο τμήμα της νέας διαδικασίας που προσανατολίζεται στην πρόσληψη.

6.5.5. Ο επίσημος ασθενής – V.I.P

Τα Επίσημα Πρόσωπα (V.I.P.) έχουν θεωρηθεί ως ευαίσθητοι ασθενείς λόγω της φύσης της σχέσης τους με το Σύστημα Υγείας (μέλη του Συμβουλίου, μέλη της οικογένειας τους), ή διότι είναι διάσημοι (αθλητές, πολιτικοί ή υψηλόβαθμοι υπάλληλοι μεγάλων οργανισμών). Οι ασθενείς που δεν είναι υπάλληλοι έχουν τη δυνατότητα περιορισμού της πρόσβασης των ηλεκτρονικών δεδομένων τους απευθυνόμενοι στο Τμήμα Ιατρικών Αρχείων και ζητώντας να τους δοθεί κατάσταση V.I.P. (Επίσημου Προσώπου). Καθώς το Τμήμα Ιατρικών Αρχείων είναι η υπηρεσία περιφρούρησης του δείκτη V.I.P., θα περιορίσει την πρόσβαση στη βάση δεδομένων ενός ασθενή λαμβάνοντας μία ενυπόγραφη αίτηση που να ζητά αυτό.

6.5.6. Ο Ασθενής – Ανακεφαλαίωση

Οι κατηγορίες των ασθενών είναι οι παρακάτω:

Κατηγορία	Πρόσβαση Ασθενή
Ασθενής του Συστήματος	Γενική Πρόσβαση Ασθενή Επιλογή 1 – Πρόσβαση Μόνο από Γιατρό
Ασθενής Υπάλληλος	Επιλογή 2 – Απαγορεύεται η Πρόσβαση σε Ηλεκτρονικό Αρχείο Επιλογή 3 – Γενική Πρόσβαση Ασθενή
Επίσημος Ασθενής (VIP)	Επιλογή 1 – Πρόσβαση Μόνο από Γιατρό Επιλογή 2 – Απαγορεύεται η Πρόσβαση σε Ηλεκτρονικό Αρχείο

Το M.I.M.S. συγκεντρώνει ηλεκτρονικά αρχεία ασθενών και λαμβάνει υπόψη του την πιθανότητα μη εξουσιοδοτημένης πρόσβασης σε αυτά. Σε αντίθεση με την αρχειοθέτηση έντυπων εγγράφων στα οποία δε γίνεται διάκριση, ο ηλεκτρονικός "πίνακας" του ασθενούς επιτρέπει την εφαρμογή ασφάλειας σε προσωπικό επίπεδο.

6.5.7. Ο πελάτης

Το MIMS αναγνωρίζει και εγκρίνει την πρόσβαση στο σύστημά της, βασιζόμενη στη λειτουργικότητα και την ανάγκη. Στις κατηγορίες πελατών συμπεριλαμβάνονται, γιατροί, ειδικευόμενοι γιατροί, υπάλληλοι του οργανισμού, φοιτητές ιατρικής, νοσοκόμες, βοηθοί γιατρών, τεχνικοί, προσωπικό ιατρικού μητρώου, επαγγελματίες υγειονομικοί υπάλληλοι, τεχνικοί εγκατάστασης μηχανογραφικού συστήματος και γενικοί χρήστες.

Η πρόσβαση στα δεδομένα επιτυγχάνεται μέσω ατομικής "Αίτησης Πρόσβασης" η οποία υποβάλλεται στο Τμήμα της Υπηρεσίας Πληροφοριών. Ζητείται από τους πελάτες να υπογράψουν μία δήλωση ασφάλειας, η οποία αποτελεί τμήμα του εντύπου της αίτησης. Η δήλωση αυτή τεκμηριώνει την Τακτική του Συστήματος Ασφάλειας έναντι της μη εξουσιοδοτημένης πρόσβασης στα αρχεία του ασθενή, καθώς επίσης και τις πιθανές πειθαρχικές επιπτώσεις σε περίπτωση ακατάλληλης χρήσης. Η δήλωση απορρήτου (1) Προσδίδει ευθύνη στον /στην πελάτη όσον αφορά τον κωδικό του /της πρόσβασης, (2) Ορίζει την ασφάλεια στην απλούστερή της μορφή (έντυπος πίνακας = ηλεκτρονικό μέσον), (3) Εισάγει την αρχή της "Ηλεκτρονικής Υπογραφής" και (4) Ορίζει τις πιθανές πειθαρχικές ποινές. Η ασφάλεια περιορισμένης πρόσβασης από ιατρικό προσωπικό εκτός Συστήματος Υγείας (η οποία εγκρίνεται κάτω από αυστηρές οδηγίες) καλύπτεται από την παρακάτω δήλωση, η οποία επίσης αποτελεί τμήμα της φόρμας αίτησης ...

Οι πελάτες εκτός Συστήματος Υγείας αποδέχονται με την υπογραφή τους, την ίδια ευθύνη απορρήτου με αυτή των υπαλλήλων του Συστήματος Υγείας και δέχονται ότι σε περίπτωση παράβασης θα γίνουν ποινικές διώξεις."

Η παρακολούθηση του αρχείου του πελάτη υπάλληλου εξασφαλίζεται με την ενδοτμηματική προώθηση δεδομένων (I.S.). Στους υπάλληλους που απολύονται αφαιρείται αυτόματα η άδεια πρόσβασης, μέσω ενημέρωσης των μισθολογικών καταστάσεων κατά την επεξεργασία των αρχείων ασφαλείας του MIMS που πραγματοποιείται κατά τη διάρκεια κάθε περιόδου πληρωμής.

Εκτός της υπογραφής ασφάλειας, μεταξύ των άλλων στοιχείων που εξετάζονται από το Συντονιστή Ασφάλειας του M.I.M.S. είναι ο αριθμός κοινωνικής ασφάλισης, η βασική θέση εργασίας, ο Κωδικός Συστήματος του γιατρού (για αιτούντες M.D.) και υπογραφή εξουσιοδότησης. Καμία υπογραφή δεν εξετάζεται εκτός αν έχει εξουσιοδότηση από τον Διευθυντή του Τμήματος του Νοσοκομείου, του διευθυντή ειδικότητας, ή του διαχειριστή της Ιστοσελίδας (site).

Η λειτουργικότητα του M.I.M.S. –μόλις εγκριθεί ο κωδικός πρόσβασης– βασίζεται στο προφίλ του πελάτη. Γιατροί, ειδικευόμενοι και υπάλληλοι έχουν πρόσβαση σε οθόνες και επιλογές του υψηλότερου επιπέδου. Η άδεια χειρισμού απορρήτων (η οποία επικυρώνεται από την επιβεβαίωση του κωδικού του γιατρού και του ονόματός του) επιτρέπει την ανάκτηση στοιχείων υπαλλήλων και επισήμων (V.I.P.). Ακόμα, η κατηγορία "Γιατρών" πελατών έχει στη διάθεσή της ορισμένες λειτουργίες που δεν προσφέρονται σε άλλους. Ιατρικές Ενδονοσοκομειακές Αναφορές, Λίστες Ασθενών και Πρακτικά Συνεδριάσεων Ιατρικών Ομάδων.

Το προσωπικό του τμήματος υγειονομικών και ιατρικών αρχείων έχει επίπεδα ασφάλειας παρόμοια με αυτά των γιατρών χωρίς τις πρόσθετες επιλογές. Αυτό το μέτρο πρόσβασης βασίζεται περισσότερο στη λειτουργικότητα της εργασίας παρά στον ιεράρχηση της περίθαλψης. Οι νοσοκόμες και το εγκεκριμένο τεχνικό προσωπικό έχουν γενική πρόσβαση (εκτός στην περίπτωση υπαλλήλων) σε όλα τα ιατρικά στοιχεία.

6.5.8. Η βάση δεδομένων

Το M.I.M.S. είναι μία αναγνώσιμη μόνο βάση δεδομένων. Είναι το αρχείο αποτελεσμάτων τα οποία καταχωρούνται στους πίνακές του από 36 βοη-θητικές πηγές, μέσω 9 πλατφόρμων συστημάτων υπολογιστών. Είναι το απο-τέλεσμα μίας πολύ προσεκτικά προγραμματισμένης στρατηγικής η οποία συν-δυάζει την αξιοπιστία των δεδομένων και την αυτονομία των τμημάτων.

6.5.9. Πρόσβαση σε στοιχεία ασθενών

Η συνεχής βάση δεδομένων S.Q.L. πληκτρολογείται σε επίπεδο ασθενή... βασικός σκοπός της είναι η περίθαλψη του ασθενή στο σημείο περίθαλψης. Διευκολύνεται η πρόσβαση με την εισαγωγή του αριθμού ιατρικού φακέλου ή του ονόματος του ασθενή.

Κάθε στοιχείο της βάσης δεδομένων (πίνακας) είναι μοναδικό ανάλογα την ιατρική ειδικότητα. Κάθε στοιχείο εφαρμόστηκε ξεχωριστά και μπορεί να τροποποιηθεί χωρίς να επηρεάσει το ένα το άλλο. Η οργάνωση των πινάκων επιτρέπει πρόσβαση σε ασθενή ή σε κατηγορία στοιχείων. Η οργάνωση της οθόνης παρουσίασης στοιχείων επιτρέπει πρόσβαση σε επίπεδο στοιχείων οθόνης.

6.5.10. Πρόσβαση στο σύνολο των στοιχείων

Συνολικά στοιχεία είναι οι γενικές πληροφορίες οι οποίες δεν αποκαλύπτουν την ταυτότητα του ατόμου και συνεπώς, δεν υπόκεινται σε περιορισμούς που επιβάλλονται από θέματα προσωπικού απορρήτου ή μυστικότητας. Οι μελέτες των τάσεων οι οποίες έγιναν σε βάσεις δεδομένων θα παίξουν πολύ σημαντικό ρόλο σε ακροατήρια ειδικευόμενων, στην ανίχνευση προβλημάτων σε πρωτογενές στάδιο και σε μελέτες σκοπιμότητας και προγραμματισμού. Το M.I.M.S., με πάνω από 270 εκατομμύρια αρχεία μέσα στα πέντε χρόνια της ιστορίας του, αποτελεί για τους ερευνητές κλινικής αποτελεσματικότητας μία ελκυστική πηγή πληροφοριών.

Η πρόσβαση στο σύνολο των στοιχείων μέσω των ήδη υπαρχόντων τρόπων παρουσίασης (format) και μεθόδων ανάκτησης (retrieval) δεν είναι δυνατή. Ο σχεδιασμός μίας βάσης δεδομένων προσδιορίζεται από την επιδιωκόμενη χρήση της. Το M.I.M.S. σχεδιάστηκε για να χρησιμοποιηθεί σε κλινικές καταστάσεις περίθαλψης οι οποίες αφορούν το ασθενή και τον νοσηλευτή. Η πρόσβαση στη βάση δεδομένων (όπως αναφέρθηκε στις προηγούμενες παραγράφους) στοχεύει κυρίως στην εξυπηρέτηση ενός ασθενή κάθε φορά. Δεν είναι δυνατόν να προσαρμοστεί με στόχο τη συγκέντρωση συνολικών στοιχείων.

6.5.11. Ευθύνη

Τέσσερα θέματα υποπίπτουν στην κατηγορία της Ευθύνης. Παρακολούθηση του τρόπου χρήσης των στοιχείων, ιδιοκτησία των στοιχείων, αναφορά και προσωπική αξιοπιστία.

6.5.11.1. Παρακολούθηση

Υπάρχει μία διαδικασία κατά την οποία οποιοσδήποτε υπάλληλος μπορεί να ζητήσει ιστορικό πρόσβασης πελάτη του M.I.M.S. στην προσωπική βάση ιατρικών δεδομένων του. Κάνοντας χρήση των πολύπλοκων ρουτινών πρόσβασης με κωδικούς (πελάτη, κατηγορίας, οθόνης, ημερομηνίας & χρόνου), το προσωπικό της Υπηρεσίας Πληροφοριών του M.I.M.S. μπορεί να δώσει έπειτα από αίτηση μία έκθεση στην οποία να φαίνεται η ημερομηνία, ή ώρα, η ταυτότητα του χρήστη και η συγκεκριμένη απεικόνιση οθόνης όλων των αιτήσεων πληροφοριών που έχουν γίνει για τον αιτούντα.

Η επεξεργασία των μεταβολών στην ιδιότητα των εργαζομένων λόγω τερματισμού της εργασίας τους στο Σύστημα Υγείας ελέγχονται αυτόματα από μία μηνιαία σύγκριση της βάσης δεδομένων των μισθολογικών καταστάσεων. Τριάντα ημέρες μετά τον τερματισμό, ένας υπάλληλος-ασθενής ταξινομείται ως μη-υπάλληλος ασθενής και τα αρχεία του είναι γενικά διαθέσιμα στο δίκτυο.

6.5.11.2. Ιδιοκτησία

Η ιδιοκτησία των δεδομένων που παρουσιάζονται στις οθόνες του MIMS ανήκει στο αρχικό σύστημα που τα παρήγαγε. "Πηγή των πληροφοριών" είναι το αυτόνομο εκείνο τμήμα ή ο ειδικός εκείνος τομέας που παρήγαγε τα στοιχεία. Όταν τα στοιχεία μεταφέρονται σε ένα άλλο τμήμα (από το LAB στο M.I.M.S.) η ευθύνη για την αξιοπιστία του ΑΝΤΙΓΡΑΦΟΥ μεταφέρεται στο σύστημα αποδοχής. Η ευθύνη για τη σωστή ΜΕΤΑΦΟΡΑ των δεδομένων βαρύνει και τα δύο συστήματα. Οι διαδικασίες επικύρωσης της μεταφοράς αφορούν την αμοιβαία συνεργασία των υπηρεσιών αποστολής και αποδοχής. Η διαδικασία μόλις εγκριθεί γραπτώς, ενεργοποιείται. Η διαδικασία επικύρωσης όχι μόνο ενεργοποιείται με την έναρξη νέας τροφοδότησης της βάσης δεδομένων... αλλά ενέχει και το συνηθισμένο, φυσιολογικό "επιχειρηματικό κόστος". Επικυρώσεις σε δεκαπενθήμερη ή και μηνιαία βάση δεν είναι ασυνήθιστες.

Ανεξάρτητα της διαδικασίας επικύρωσης, επιβάλλεται μία ακόμα επαλήθευση των δεδομένων πριν την εφαρμογή τους σε ένα συγκεκριμένο Αριθμό Ιατρικού Αρχείου (MRN) του MIMS. Τα ψηφία του ονόματος των μεταφερόμενων δεδομένων πρέπει να ταιριάζουν με αυτά του βασικού δείκτη ασθενή MIMS, τα οποία δίνουν δημογραφικές πληροφορίες του ασθενή. Χωρίς αυτή την επαλήθευση (MRN = MRN και Όνομα = Όνομα), τα δεδομένα δεν γίνονται αποδεκτά στο αρχείο.

6.5.11.3. Αναφορά

Τα δεδομένα τα οποία περιέχονται σε ένα αρχείο ιατρικών δεδομένων είναι περισσότερο εμπιστευτικά από ότι τα στοιχεία τα οποία μπορούν να αποκομιστούν από βάσεις δημογραφικών δεδομένων. Αν ο ορισμός των συνολικών στοιχείων ως "γενικών πληροφοριών" εφαρμόζονταν σε περιπτώσεις ιατρικών ηλεκτρονικών δεδομένων, η απόφαση ελεύθερης πρόσβασης στη βάση δεδομένων θα είχε δοθεί από την αρχή της δημιουργίας της. Το MIMS όμως δεν "καλύπτει" τους ασθενείς του ... η αναφορά συγκεντρωτικών στοιχείων δεν αποτελεί προμελετημένο όφελος. Η ανωνυμία είναι ευάλωτη.

Η εκούσια ή ακούσια λανθασμένη ερμηνεία των ευαίσθητων υγειονομικών πληροφοριών μπορεί να έχει καταστροφικές συνέπειες για ορισμένες υποομάδες ασθενών, εργαζόμενους στο σύστημα υγειονομικής περίθαλψης, το Ίδρυμα και άμεσα ή έμμεσα εμπλεκόμενα ιδρύματα ή άτομα. Για αυτό το λόγο, συγκεντρωτικά στοιχεία είναι επί του παρόντος διαθέσιμα μόνο μέσω ελεγχόμενων διαδικασιών για ερευνητικούς σκοπούς. Εκθέσεις οι οποίες προστατεύουν το απόρρητο των ασθενών εκδίδονται, αλλά δεν έχουμε μεταφορά ή διάθεση ΣΤΟΙΧΕΙΩΝ μέσω δικτύου υπολογιστών ή με άλλο μηχανικό τρόπο.

Το Σύστημα Υγείας έχει δημιουργήσει μία επίσημη διαδικασία με την οποία θα προσδιορίζονται τα όρια της πρόσβασης και διανομής των συγκεντρωτικών στοιχείων στο μέλλον. Καθώς η ανάκτηση αυτού του τύπου δεδο-

μένων θα έχει επιπτώσεις στην απόδοση του συστήματος, το απόρρητο του ασθενή και σε θέματα ιδιοκτησίας των δεδομένων, έχει δημιουργηθεί ένα διοικητικό σώμα για την καθιέρωση στρατηγικών του Συστήματος Υγείας, πάνω σε έξι βασικά θέματα: Ασφάλεια, πρόσβαση, αίτηση, έγκριση, ανάκτηση και παροχή δεδομένων.

6.5.11.4. Προσωπική Ακεραιότητα

Αυτή η κατηγορία υπευθυνότητας είναι εκείνο το στοιχείο για ένα σύστημα ασφαλείας το οποίο μπορεί να παρακάμψει και να καταργήσει ακόμα και τα πιο "προσεκτικά προετοιμασμένα σχέδια". Δεν υπάρχει σύστημα παρακολούθησης, τοπικός έλεγχος δικτύου, ούτε επακόλουθη έκθεση που να μπορεί να αστυνομεύσει την ακεραιότητα του πελάτη, ή να προφυλάξει σε περίπτωση απουσίας της. Ακόμα και στην περίπτωση της εκπαίδευσης, σε επίπεδο χρήστη, τα μέσα θα δικαιωθούν από το αποτέλεσμα.

Ένα μέλος του προσωπικού θα "Παραχωρήσει" τον κωδικό πρόσβασής της σε κάποιο συνεργάτη.

Ένας γιατρός θα δώσει τη λειτουργία πρόσβασής του στο Βοηθό του ο οποίος παρακολουθεί τους ασθενείς του.

Ένας πελάτης θα ελέγξει τα Εργαστηριακά αποτελέσματα της μητέρας του πριν το ραντεβού.

Ένας γείτονας θα ψάξει τα αρχεία των συγκατοίκων της πολυκατοικίας του.

Ένας υπάλληλος θα αναζητήσει στοιχεία άλλων υπαλλήλων στο δίκτυο.

Η εκπαίδευση με σκοπό την προστασία έναντι κακή χρήση της πρόσβασης και "πειθαρχικές κυρώσεις" για αυτούς που αρνούνται να συμμορφωθούν μπορεί να μην λύσουν το πρόβλημα της ακεραιότητας.

Παρόμοιες παραβάσεις της ασφάλειας και του απορρήτου συμβαίνουν καθημερινά. Ο καιροσκόπος θα εκμεταλλευτεί την ευκαιρία.

Ένα σύστημα ηλεκτρονικών υπολογιστών μπορεί να προειδοποιήσει, να παρακολουθήσει και να απομονώσει σε μία προσπάθεια επιβολής ασφάλειας, αλλά αυτός που τελικά πρέπει να την ενισχύσει είναι ο πελάτης.

6.6. Συμπέρασμα

Η ασφάλεια είναι ένα αγαθό το οποίο απαιτεί άγρυπνη επιφυλακή. Οι προσδοκίες θα πρέπει να ισχυροποιηθούν με ρεαλισμό... με δεδομένη την αδυναμία οποιουδήποτε ηλεκτρονικού υπολογιστή να υπερνικήσει την έλλειψη επαγγελματισμού που επιδεικνύουν μερικοί χρήστες του συστήματος.

Η αναγνώριση των πελατών του συστήματος, ο περιορισμός της πρόσβασής τους ανάλογα με τις "ανάγκες" και η παρακολούθηση της πρόσβασης των χρηστών στην μηχανογραφημένη, ιατρική βάση δεδομένων, είναι σίγουρα στοιχεία απαραίτητα ακόμα και για να έχουμε στοιχειώδη μόλις ασφάλεια.

Η απουσία εθνικών και πολιτειακών νόμων οι οποίοι θα όριζαν ή θα ρύθμιζαν τη χρήση των ηλεκτρονικών ιατρικών μέσων, επιβάλλει στα ινστιτούτα ιατρικής περίθαλψης να αντιμετωπίσουν το πρόβλημα του απόρρητου των ασθενών και της ασφάλειας δεδομένων με λογική και προσοχή... λογική η οποία θα υπαγορεύει ότι η Ουτοπία δεν είναι δυνατόν να επιτευχθεί και προσοχή η οποία θα δίνει έμφαση σε σενάρια λιγότερο απαισιόδοξα από αυτά της "χειρότερης περίπτωσης".

Τα μέτρα αυτά θα αποτελέσουν τους θεμέλιους λίθους με τους οποίους θα αντιμετωπιστεί το πρόβλημα της πρόσβασης σε ένα δικτυακό ηλεκτρονικό σύστημα το οποίο δημιουργείται από μία κοινότητα και /ή από τοπικά δίκτυα. Η προσοχή με την οποία αυτά τα μέτρα εφαρμόζονται και χρησιμοποιούνται θα προσδιορίσει το βαθμό ως προς τον οποίο ο γενικός πληθυσμός αποδέχεται τα ηλεκτρονικά μέσα σαν ένα αναπόσπαστο τμήμα του συστήματος ιατρικής περίθαλψης.

6.7. Τεχνολογίες Διαδικτύου

6.7.1 Το διαδίκτυο καταλαμβάνει τον τομέα υγειονομικής περίθαλψης

Σήμερα σύγχρονη εποχή μικρών αντιστάσεων εισαγωγής και μεγάλης επενδυτικής ενέργειας, οι καταναλωτές οδηγούν τις επενδύσεις σε νέες εταιρείες και προϊόντα πρωτόγνωρα στο χώρο της υγείας.

Οι καταναλωτές βλέπουν την υγειονομική περίθαλψη ως ένα γερασμένο, εσωστρεφή τομέα ο οποίος με κάθε ευκαιρία παρατάσσει εμπόδια στην παροχή υπηρεσιών, από πολύπλοκες φόρμες οι οποίες δίνουν την εντύπωση ότι δεν θα μπορέσουν ποτέ να συμπληρωθούν, έως τους μεγάλους χρόνους αναμονής, την απρόθυμη αντιμετώπιση κατά την ιατρική επίσκεψη και τις βιαστικές μπερδεμένες οδηγίες των γιατρών. Το σύστημα υγειονομικής περίθαλψης μόλις έχει αρχίσει να βλέπει τους ασθενείς ως καταναλωτές έπειτα από πολλές δεκαετίες κατά τις οποίες ήταν υπόλογο σε προγράμματα υγείας, οργανισμούς διαχείρισης περίθαλψης και υπαλλήλους που "πλήρωναν τα σπασμένα". Αλλά η συνειδητοποίηση του συστήματος υγείας είναι αποτέλεσμα κυρίως των ίδιων των ασθενών που το απαίτησαν.

Ο Steve O' Dell, αντιπρόεδρος και διευθύνων σύμβουλος της Ηλεκτρονικής Υγειονομικής Πρακτικής του F.C.G. δήλωσε: "Αν είχα τη δυνατότητα ενεργοποίησης του συστήματος υγειονομικής περίθαλψης με το πάτημα ενός κουμπιού – ενός κουμπιού που να το παρείχε η τεχνολογία – τότε αυτό θα αποτελούσε επανάσταση για τον καταναλωτή. Στο παρελθόν μιλούσαμε για κάτι τέτοιο, αλλά αυτό τελικά θα γίνει πραγματικότητα χάρη στο διαδίκτυο."

Οι O' Dell και ο Chris McGoldrick, διευθυντής της ομάδας νέων πρακτικών του F.C.G., έχουν συντάξει μία λίστα δέκα τάσεων οι οποίες πιστεύουν ότι θα μεταμορφώσουν τη βιομηχανία υγειονομικής περίθαλψης. Στη λίστα αυτή συμπεριλαμβάνονται νέες αντιλήψεις όπως ότι "το Περιεχόμενο σαν μία αυτόνομη δραστηριότητα έχει περιοριστεί" (εννοώντας ότι όλα

τα χρήματα τα οποία χορηγούνται στις υπηρεσίες συγκέντρωσης πληροφοριών υγειονομικής περίθαλψης θα πάνε χαμένα, εκτός αν οι διαδικτυακές πύλες προσφέρουν υπηρεσίες επί αμοιβή). Οι περισσότερες όμως από τις τάσεις που προσδιορίζουν καθοδηγούνται ή επηρεάζονται από – μαντέψτε ποιους – τους καταναλωτές!

"Έχουμε διαπιστώσει ότι οι παραδοσιακοί παίκτες τη αγοράς – I.D.N., κ.ά. – δεν ικανοποιούν τις ανάγκες των καταναλωτών, δηλώνει ο McGoldrick. Ο O' Dell συμφωνεί. "Ο κόσμος νομίζει ότι όλοι καταφεύγουν στο διαδίκτυο για να συλλέξουν (ιατρικής φύσεως) πληροφορίες, αλλά οι μόνοι που ενδιαφέρονται είναι εκείνοι οι οποίοι έχουν κάποιο πρόβλημα υγείας, ή κάποιο άλλο μέλος της οικογένειάς τους. Θα δούμε όλο και περισσότερες ομάδες ασθενών όπως αυτές που καθοδηγούν την έρευνα, οι οποίες θα διαπιστώνουν τις εξελίξεις και τις σημαντικές και χρήσιμες πληροφορίες, ιδίως σε περιπτώσεις χρόνιων καταστάσεων οι οποίες δεν αντιμετωπίζονται ικανοποιητικά από το σύστημα υγειονομικής περίθαλψης.."

Τι γίνεται όμως όσον αφορά το κόστος; Μήπως όλη αυτή η πρόσβαση στις πληροφορίες αυξήσει τη ζήτηση ιατρικών υπηρεσιών;

Ο O' Dell δηλώνει: "Ο κόσμος νομίζει ότι όλοι επιζητούν συνεχώς όσο δυνατόν περισσότερα. Αυτό όμως δεν είναι αλήθεια. Πολλοί απορρίπτουν τις μεταμοσχεύσεις μόλις συνειδητοποιήσουν τι συμπεριλαμβάνουν. Δεν πιστεύω ούτε για μία στιγμή ότι οι απαιτήσεις του κόσμου όσον αφορά την υγειονομική περίθαλψη είναι ακόρεστες."

Ο McGoldrick συμφωνεί: "Καθώς οι καταναλωτές πληρώνουν όλο και περισσότερα για την υγειονομική τους περίθαλψη, οι αποφάσεις τους επηρεάζονται και από αυτό τον παράγοντα επίσης."

Ο Graham Pallett, συνεργάτης της Deloitte Consulting, είναι μέρος μίας ερευνητικής προσπάθειας η οποία βρίσκεται σε εξέλιξη στο Deloitte με σκοπό την ανάλυση της επίδρασης αυτού που ονομάζει "καταναλωτές ηλεκτρονικής υγειονομικής φροντίδας" στην υγειονομική φροντίδα και τον προσδιορισμό των απαραίτητων εκείνων παραγόντων που πρέπει να διαθέτουν οι οργανισμοί για να τους ικανοποιήσουν. Συμφωνεί ότι οι καταναλωτές λαμβάνουν υπόψη το κόστος και ότι αναμένουν στο μέλλον να πληρώνουν περισσότερα και να λαμβάνουν λιγότερα. Οι συμμετέχοντες στην πρώτη φάση της έρευνας Deloitte /Cyber Dialogue η οποία μόλις κοινοποιήθηκε, στην ερώτηση για ποιες υπηρεσίες θα πλήρωναν ευχαρίστως περισσότερα, απάντησαν ότι θα πλήρωναν για ευκολίες όπως δυνατότητα επικοινωνίας μέσω διαδικτύου με το πρόγραμμα υγειονομικής τους περίθαλψης και τους γιατρούς τους.. Λίγοι απάντησαν ότι θα πλήρωναν οτιδήποτε για περιεχόμενο – το επίκεντρο δηλαδή έντονης επενδυτικής δραστηριότητας και δημιουργίας μεγάλου αριθμού ιστοσελίδων σε θέματα περίθαλψης τα τελευταία δύο χρόνια.

"Οι καταναλωτές λένε ότι θα πλήρωναν περισσότερα για ευκολίες όπως δυνατότητα επικοινωνίας μέσω διαδικτύου με τους γιατρούς και για τρόπους αποφυγής των επισκέψεων στους γιατρούς" λέει ο Pallett. "Ποιος είναι λοιπόν ο λόγος εισαγωγής περιεχομένου στο διαδίκτυο; Αν εκπροσωπείς

μία από τις 25.000 ιστοσελίδες που βρίσκονται σε αυτό, τι είναι αυτό που σε διαφοροποιεί από τις υπόλοιπες; Οι διαδικτυακές στρατηγικές θα πρέπει να προσανατολιστούν περισσότερο στην παροχή ευκολιών και λιγότερο στην παροχή περιεχομένου."

Οι διοικητικοί υπάλληλοι και οι εμπορικές εταιρείες της βιομηχανίας μπορούν τώρα να εστιάσουν την προσοχή τους στους τρεις παράγοντες της στρατηγικής διαδικτύου (τα τρία C – content, connectivity, commerce – περιεχόμενο, συνδεσιμότητα, εμπόριο), αλλά ο βασικός παράγοντας (το μεγάλο C - consumers) - οι καταναλωτές – έχουν μερικά δικά τους κριτήρια. Αυτά είναι οι παρεχόμενες ευκολίες, το κόστος και η σιγουριά.. Έτσι, ενώ οι αλλαγές στον τομέα υγειονομικής περίθαλψης καθοδηγούνται από τον καταναλωτισμό του διαδικτύου, τα παραπάνω κριτήρια θα είναι με τη σειρά τους τα μέτρα που καθοδηγούν τους καταναλωτές.

Αν δεν είναι ήδη μέρος της δικής σας διαδικτυακής στρατηγικής σας, θα είναι στο μέλλον.

6.8. Οι εμφανιζόμενες τάσεις ηλεκτρονικής περίθαλψης σύμφωνα με την First Consulting Group – F.C.G.

1. Η μη ιδιοκτησιακή συσσώρευση περιεχομένου σαν μία αυτόνομη δραστηριότητα έχει συρρικνωθεί. Οι διαδικτυωμένες εταιρείες με βασική πηγή εσόδων την διαφήμιση, σε μία προσπάθεια να επιβιώσουν έχουν αναγκαστεί να αναθεωρήσουν τα επιχειρησιακά τους μοντέλα. Το περιεχόμενο αυτού του είδους αφθονεί και για να αναπτυχθούν οικονομικά οι υπηρεσίες παροχής περιεχομένου θα πρέπει να μεταβληθούν σε κάτι περισσότερο από "χορηγούς πληροφοριών." Οι εταιρείες αυτές είτε συγχωνεύονται ή προσπαθούν να μετατραπούν σε οργανισμούς που ειδικεύονται σε θέματα όπως είναι η διαχείριση των ασθενειών και οι κλινικές εξετάσεις. Θα πρέπει να αναμένουμε συνεχείς συγχωνεύσεις καθώς οι παίκτες της αγοράς προσπαθούν να αγοράσουν το απαραίτητο εκείνο εύρος δέσμης συχνοτήτων για να διευρύνουν τις επιχειρήσεις τους.

2. Αν και ο τομέας συνδεσιμότητας και εμπορικής συναλλαγής της αγοράς συγχωνεύεται ταχύτατα, παρόλα αυτά η δημιουργία δέσμης λύσεων και σταθερών επιχειρηματικών μοντέλων παραμένει μία απατηλή υπόσχεση. Οι οργανισμοί υγειονομικής περίθαλψης δεν διαθέτουν το χρόνο και τους πόρους που απαιτούνται για τη δημιουργία προσαρμοσμένων λύσεων συναλλαγών, αλλά επιζητούν την αξία που υπόσχονται αυτές οι λύσεις με σκοπό την επιστροφή στην γραμμή αναφοράς. Η Healtheon/WebMD, μέσω αγορών υψηλού προφίλ, έχει αυτοπροσδιοριστεί ως πρότυπο, με δυνατότητα πλέον να γίνει η Microsoft του συγκεκριμένου τομέα της αγοράς. Θα πρέπει να αναμένουμε περαιτέρω συγχωνεύσεις σε

αντίδραση των κινήσεων της Healtheon/WebMD καθώς δραστηριοποιείται για την ενσωμάτωση των πρόσφατων αποκτημάτων της.

3. Η ηλεκτρονική μετατροπή του τομέα υγειονομικής περίθαλψης δεν έχει ακόμα επηρεάσει τους οργανισμούς παροχής υπηρεσιών ή τους ασφαλισμένους. Οι οργανισμοί παροχής υγειονομικής περίθαλψης διακρίνουν την πιθανή αξία που μπορεί να προσθέσει το διαδίκτυο στις επιχειρήσεις τους. Σε μία πρόσφατη έρευνα μεταξύ διοικητικών υπαλλήλων ηλεκτρονικών υπηρεσιών υγειονομικής περίθαλψης κορυφαίων προγραμμάτων, η F.G.C. διαπίστωσε ότι σχεδόν το 80% θεωρούν ότι τα προγράμματα θα ωφεληθούν από το διαδίκτυο, ομαλοποιώντας τις διαδικασίες τους. Λίγοι όμως έχουν δραστηριοποιηθεί προς αυτή την κατεύθυνση. Διαπιστώσαμε ότι η βιομηχανία βρίσκεται ακόμα σε ένα πρωτογενές στάδιο υιοθέτησης του διαδικτύου. Η πραγματική του αξία δεν έχει ακόμα αναδειχθεί. Η ενσωμάτωση του διαδικτύου στις ήδη υπάρχουσες εφαρμογές και διαδικασίες θα αποτελέσει το βασικό στόχο, η επίτευξη ή όχι του οποίου θα διαχωρίσει τους νικητές από τους ηττημένους.

4. Η ηλεκτρονική μετατροπή της διαδικασίας διαχείρισης παροχής υπηρεσιών θα αποτελέσει τη βάση για τη μελλοντική ηλεκτρονική μετατροπή της διαδικασίας περίθαλψης. Οι οργανισμοί παροχής υπηρεσιών υγειονομικής περίθαλψης θα ωφεληθούν πολύ από την αυτοματοποίηση των διαδικασιών διαχείρισης παροχής. Η υγειονομική περίθαλψη, ως μία βιομηχανία, θα πρέπει να υπερνικήσει πιο σημαντικά θέματα στον τομέα της υγειονομικής διαχείρισης: Θα πρέπει να εξασφαλίσει μείωση των ιατρικών σφαλμάτων και εντατικοποίηση εφαρμογής αποδεδειγμένων πρακτικών. Αυτός είναι και ο τομέας όπου μπορούμε να πετύχουμε πραγματικές βελτιώσεις σε θέματα κόστους και ποιότητας, βελτιώσεις οι οποίες θα επισκιάσουν την αξία που δεσμεύει η αυτοματοποίηση των διαδικασιών παροχής υπηρεσιών. Το δυναμικό του διαδικτύου όσον αφορά τη μεταβολή της σχέσης μεταξύ των ασθενών και των υπηρεσιών περίθαλψης μέσω ανταλλαγής γνώσεων και πληροφοριών θα επιφέρει σημαντική και διαρκή επίδραση στην παροχή υγειονομικής περίθαλψης.

Παραμένει όμως το κρίσιμο ερώτημα: Θα μπορέσουν αυτές οι μέθοδοι να αποφέρουν αξία και να γίνουν αποδεκτές από τους νοσοκομειακούς γιατρούς; Οι φορητοί υπολογιστές είτε αποτελούν το τελευταίο ή ένα ενδιάμεσο στάδιο, θα επιταχύνουν την εισαγωγή των γιατρών στην επανάσταση της ηλεκτρονικής υγειονομικής περίθαλψης.

5. Η υπερβολική διαμεσολάβηση (σε αντίθεση με την απουσία διαμεσολάβησης) θα δημιουργήσει την ανάγκη δημιουργίας υπηρεσιών καθοδήγησης (navigator). Ο Nicholas Carr εισήγαγε τον όρο υπερβολική διαμεσολάβηση και επισήμανε το γεγονός ότι οι "διαμεσολαβητές" δεν έχουν εκλείψει αλλά αντικατασταθεί από μία ομάδα "αόρατων" παικτών οι οποίοι καραδοκούν πίσω από την "ηλεκτρονική κουρτίνα." Καθώς τα αναγνωρίσιμα από τους καταναλωτές στοιχεία περνούν από τα χέρια τους (ή από τους διακομιστές), η τάση αυτή εγείρει σημαντικά ερωτήματα αναφορικά με το απόρρητο των προσωπικών πληροφοριών και την εμπιστοσύνη των καταναλωτών στις εταιρείες, θέματα τα οποία η βιομηχανία θα πρέπει να αντιμετωπίσει - κάτι που ενισχύεται βάσει της πρόσφατης έρευνας της F.T.C. στις επιχειρηματικές πρακτικές της "DoubleClick." Το ερώτημα που παραμένει αναπάντητο είναι ποια θα είναι η υπηρεσία καθοδήγησης εκείνη που θα εμπιστεύεται ο καταναλωτής με την πληθώρα των διαμεσολαβητών που υπάρχουν ήδη; Το πιθανότερο είναι ότι θα προέλθει από ομάδες ασθενών /καταναλωτών με κοινά ενδιαφέροντα (π.χ., ηλικία, χρόνια κατάσταση)[2].

6. Η απαίτηση των καταναλωτών για συνδεσιμότητα και επικοινωνία με τις υπηρεσίες υγειονομικής περίθαλψης και τις ασφαλιστικές. Οι καταναλωτές έχουν συγκεκριμένες προσδοκίες όσον αφορά σε τι και σε ποιους θα έχουν πρόσβαση μέσω του διαδικτύου. Σήμερα, αυτές οι προσδοκίες δεν καθορίζονται από τον ανταγωνισμό, αλλά από τις ηλεκτρονικές παρασιτικές υπηρεσίες και τους οργανισμούς οικονομικών υπηρεσιών. Οι καταναλωτές θα παίρνουν τις αποφάσεις τους όσον αφορά τις αγορές τους όλο και περισσότερο βάσει της πρόσβασης που θα τους χορηγείται και του επιχειρηματικού βαθμού ευκολίας διεκπεραίωσης των υποθέσεών τους. Συνεπώς, οι υπηρεσίες παροχής υπηρεσιών περίθαλψης και οι ασφαλιστικές θα αναγκαστούν να βελτιώσουν τα τρέχοντα επίπεδα προσωπικής αντιμετώπισης και επικοινωνίας. Εκείνοι που δεν θα το πράξουν θα θέσουν σε κίνδυνο το μερίδιο αγοράς τους.

7. Θα εμπιστευτούμε το δικτυακό περιεχόμενο υγειονομικής περίθαλψης και τις εταιρείες διασύνδεσης όταν Κύριος του Διαδικτύου γίνει ο Δαλάι Λάμα το έτος 2077. Η προστασία των προσωπικών δεδομένων και η ασφάλεια καθίστανται όλο και περισσότερο το βασικό εμπόδιο υιοθέτησης της διαδικτυακής τεχνολογίας στο χώρο της υγειονομικής περίθαλψης. Θα πρέπει να αντιμετωπιστούν οι βαθιά ριζωμένοι προβληματισμοί των καταναλωτών. Η πρόκληση έγκειται στο να κατανοήσουμε πότε οι προβληματισμοί σε θέματα προσωπικών δεδομένων και ασφάλειας είναι εύλογοι και πότε αποτελούν απλώς μία δικαιολογία αντίστασης στην εξέλιξη.

8. Η μεταβίβαση της αγοράς της ασφάλειας από τον εργοδότη θα αποτελέσει το βασικό ερέθισμα για την έκρηξη του καταναλωτισμού και την ανάδειξη της αγοράς πρόσωπο με πρόσωπο στο χώρο της υγειονομικής περίθαλψης. Οι καταναλωτές όχι μόνο θα περιμένουν αξία και

υπηρεσίες από τους επίδοξους ασφαλιστές, αλλά θα εξετάζουν εξονυχιστικά τα έξοδα που αφορούν θέματα υγείας, καθώς θα αρχίσουν να συσχετίζουν το κόστος της περίθαλψης με την προσωπική οικονομική τους κατάσταση. Οι ασφαλιστές και οι υπηρεσίες παροχής περίθαλψης θα πρέπει να δώσουν έμφαση στην πιο προσωπική συναλλαγή και χορήγηση υπηρεσιών.

Η Γραμμή Αναφοράς. Τελευταία γίνεται πολύς λόγος για την Ηλεκτρονική Υγεία αλλά τα έργα σε αυτόν τον τομέα παραμένουν λίγα και συνεπώς η αξία που αποκομίζεται παραμένει μικρή. Το διαδίκτυο παραμένει μία σχετικά ανεκμετάλλευτη ευκαιρία για τη βιομηχανία. Η επιτυχία θα έρθει έπειτα από πολύ μεγάλες δαπάνες, καθώς οι συμμετέχοντες θα βασίζουν την υποδομή, τους οργανισμούς, τις διαδικασίες και εφαρμογές τους στο διαδίκτυο και θα αρχίζουν να αποκομίζουν την αξία των επενδύσεών τους στην Ηλεκτρονική Υγεία.

6.9. Ο όμιλος TriZetto προσφέρει λύσεις οι οποίες βοηθούν τον κλάδο υγειονομικής περίθαλψης να ομαλοποιήσει τις επιχειρηματικές του διαδικασίες.

Εισαγωγή.

Ο Όμιλος Trizetto Inc., ηγείται στον τομέα παροχής υπηρεσιών διαδικτυακών εφαρμογών, επιχειρησιακών πυλών και εφαρμογών διαδικτύου για τη βιομηχανία υγειονομικής περίθαλψης. Τον Οκτώβριο του 1999Ο ο Όμιλος Trizetto έγινε μία εταιρεία δημόσιων συναλλαγών, με μία ομάδα διαχείρισης η οποία διαθέτει κατά μέσο όρο 14 χρόνια εμπειρίας στο χώρο της τεχνολογίας πληροφορικής της βιομηχανίας υγειονομικής περίθαλψης. Η Trizetto σήμερα έχει 14 μεγάλα γραφεία στις Η.Π.Α. και απασχολεί 700 περίπου υπαλλήλους. Η εταιρεία επί του παρόντος προσφέρει υπηρεσίες σε πάνω από 140 οργανισμούς υγειονομικής περίθαλψης, συμπεριλαμβανομένων ασφαλειών, υπηρεσιών και διαχειριστών επιδομάτων.

Ο τομέας υγειονομικής περίθαλψης παραδοσιακά επενδύει σημαντικό χρόνο και κεφάλαιο στην ανάπτυξη, διατήρηση, ανάλυση και διακίνηση πληροφοριών. Τελευταία η βιομηχανία βρίσκεται σε μία καμπή. Σε ένα σημείο όπου η χρήση της τεχνολογίας της πληροφορικής (Ι.Τ.) αυξάνεται και όπου η μείωση του κόστους αποτελεί σημαντική επιδίωξη. Αυτό σημαίνει ότι πολλοί οργανισμοί προσπαθούν να βρουν τρόπους να ομαλοποιήσουν τη χρήση πληροφοριών και της τεχνολογίας που την υποστηρίζει. Η βασική ιδέα είναι η βελτιστοποίηση των εργασιακών διαδικασιών χωρίς να επηρεάζεται αρνητικά η κερδοφορία ή η περίθαλψη που προσφέρεται στους ασθενείς.

Για τη διατήρηση των δυνατοτήτων της Τεχνολογίας της Πληροφορικής (IT) και των σχέσεων με άλλους συμμετέχοντες στην αλυσίδα αξίας της υγειονομικής περίθαλψης, περιορίζοντας παράλληλα το κόστος, πολλές υπηρεσίες, ασφάλειες και διαχειριστές επιδομάτων απευθύνονται στον Όμιλο TriZetto. Οι χαρακτηριστικές διαδικτυακές λύσεις της εταιρείας προσφέρουν σε αυτές τις ομάδες την δυνατότητα να εξασφαλίσουν υψηλά λειτουργικά επίπεδα, ελαχιστοποιώντας παράλληλα το κόστος.

Η TriZetto επικεντρώνει την προσπάθειά της στη δημιουργία πολλών ευκαιριών για τους οργανισμούς παροχής υγειονομικής περίθαλψης. Ο Lu Kabir, ανώτερος αντιπρόεδρος μάρκετινγκ και επιχειρησιακής ανάπτυξης της TriZetto δηλώνει: "Ενεργούμε ως υπηρεσία εφαρμογών (ASP), η οποία παρέχει λογισμικό αιχμής, το καλύτερο στην κατηγορία του, σε εταιρείες – τρίτα μέρη – οι οποίες το χρειάζονται για να λειτουργήσουν επιχειρηματικά. Εκτός της προσέγγισης ASP, διατηρούμε και προωθούμε επίσης την πρώτη διαδικτυακή επιχειρηματική πύλη η οποία απευθύνεται σε επιχειρήσεις, ενώ προωθούμε ακόμα και εφαρμογές οι οποίες επιτρέπουν στις επιχειρήσεις να διεκπεραιώνουν τις ηλεκτρονικές επιχειρηματικές τους δραστηριότητες και να έχουν πρόσβαση σε πολλές σημαντικές υπηρεσίες."

Καθιστώντας τις Βασικές Εφαρμογές (Core Applications) πιο Αποτελεσματικές

Ως υπηρεσία εφαρμογών (ASP) η TriZetto προσφέρει εφαρμογές οι οποίες διευκολύνουν τις εταιρείες στην παροχή των οικονομικών τους υπηρεσιών, στις διαδικασίες πληροφόρησης και αναφοράς, στα συστήματα διαχείρισης πρακτικών και την ανάλυση δεδομένων. Οι εφαρμογές αυτές μπορούν ακόμα να προσφέρουν σε ομάδες γιατρών ένα τρόπο διερεύνησης πληροφοριών ασθενών και υποβολής αιτήσεων. Η βασική ιδέα λέει ο Kabir, είναι η αύξηση της αποδοτικότητας. "Προσφέροντας βασικές εφαρμογές επιχειρησιακού γραφείου, έχουμε τη δυνατότητα να μεταπηδήσουμε από το υπάρχον περιβάλλον και να συμβάλλουμε στην εξοικονόμηση κεφαλαίου και χρόνου εφαρμογής και να μειώσουμε το συνολικό κόστος που σχετίζεται με τη λειτουργία και διαχείριση πολύπλοκων επιχειρηματικών εφαρμογών."

Η συνεργασία με ηγετικές εταιρείες ανάπτυξης λογισμικού βοηθά την TriZetto να το πετύχει. Επί του παρόντος παρέχει εφαρμογές όπως Amysis, PenChart, Epic, Medic, Raintree, QCSI, InfoMetrics, WellMed και Great Plains.

Δυνατότητα Απεριόριστης Συνδεσιμότητας

Η TriZetto, με την πύλη που διαθέτει με την ονομασία HealthWeb και με την υποστήριξη αρχιτεκτονικής ηλεκτρονικής επιχείρησης, έχει τη δυνατότητα να εστιάσει το πεδίο εργασίας ενός επαγγελματία του τομέα υγειονομικής περίθαλψης σε ένα διαδικτυακό περιβάλλον υπολογιστή γρα-φείου. "Η πύλη HealthWeb είναι η μόνη διαδικτυακή φιλική προς το χρήστη λύση η

οποία παρέχει ότι χρειάζεται για την πραγματοποίηση τυπικών εργασιών" εξηγεί ο Kabir.

Η HealthWeb προσφέρει εφαρμογές εσωτερικής διαχείρισης αλλά και υπηρεσίες εφαρμογών, δημιουργώντας έτσι ένα δυναμικό περιβάλλον εργασίας με ανυπέρβλητες δυνατότητες πρόσβασης. Μεταξύ των διοικητικών υπηρεσιών συμπεριλαμβάνονται επαγγελματικές εφαρμογές παραγωγικότητας, προγραμματισμός και εξουσιοδότηση διαδικασιών, καθώς και άλλες επιχειρησιακού τύπου εργασίες οι οποίες πραγματοποιούνται μέσω ενός περιβάλλοντος διασύνδεσης παρόμοιου με αυτό πυλών όπως του Yahoo! και της America Online. Έχοντας πρόσβαση από τον υπολογιστή γραφείου σε διαδικτυακές πηγές υγειονομικής περίθαλψης, οι χρήστες μπορούν να πραγματοποιήσουν εξειδικευμένη έρευνα, να έχουν πρόσβαση σε κωδικοποιημένες κλινικές πληροφορίες, να ανατρέχουν σε οδηγίες του Αμερικανικού Ιατρικού Συλλόγου (American Medical Association), να λαμβάνουν έκτακτα δελτία ειδήσεων από αξιόπιστες πηγές, ή να διερευνούν τρέχοντα ή αρχειοθετημένα ιατρικά περιοδικά. Οι ενσωματωμένες δυνατότητες ηλεκτρονικού εμπορίου επιτρέπουν στους χρήστες να πραγματοποιούν επιχειρηματικές συναλλαγές μέσω του διαδικτύου, ψάχνοντας καταλόγους και κάνοντας αγορές από το τερματικό του ηλεκτρονικού υπολογιστή τους.

"Η βασική ιδέα πίσω από την HealthWeb ήταν να διαθέσουμε το ηλεκτρονικό εμπόριο και τις υπόλοιπες υπηρεσίες στους διαχειριστές και τη διοίκηση των οργανισμών υγειονομικής περίθαλψης, έτσι ώστε να έχουν ένα προσωπικό περιβάλλον το οποίο να τους βοηθά να εργάζονται καλύτερα και ταχύτερα," εξηγεί ο Kabir. "Η πρόσβαση από ένα ή περισσότερα σημεία, έχει αποδειχθεί ότι είναι ένας πολύ αποτελεσματικός τρόπος βελτιστοποίησης της ευελιξίας." Η TriZetto προσφέρει ακόμα Υπηρεσίες Μετατροπής, σχεδιασμένες κατά τέτοιο τρόπο ώστε να βοηθούν τις εταιρείες να καθορίζουν ένα τρόπο δράσης και να εφαρμόζουν λύσεις με σκοπό τη βελτιστοποίηση της χρήσης της τεχνολογίας τους. Και ο Kabir προσθέτει: "Οι Υπηρεσίες Μετατροπής TriZetto αποτελούνται από μία ομάδα κατάλληλων επαγγελματιών οι οποίοι βοηθούν τις εταιρείες να κατανοήσουν ποιες είναι οι ανάγκες τους σε θέματα τεχνολογίας, αλλά και πως να εφαρμόσουν αυτή την τεχνολογία. Αυτό αποτελεί μέρος της όλης μας προσέγγισης, η οποία αποσκοπεί στο να βοηθήσουμε αυτούς τους οργανισμούς να ευθυγραμμίσουν τις πρωτοβουλίες Τεχνολογίας Πληροφορικής (IT) με τους επιχειρηματικούς τους στόχους."

Κάνοντας τις Λύσεις να Δουλεύουν για Όλους

Ο Kabir πιστεύει ότι τελικά, μοντέλα όπως αυτά θα υιοθετηθούν από τους οργανισμούς υγειονομικής περίθαλψης όλων των μεγεθών σε μία προσπάθεια βελτίωσης των βασικών στρατηγικών τους σε σύντομο χρονικό διάστημα και διατήρησης ή αύξησης της ανταγωνιστικότητάς τους. "Έχουμε μερικούς μεγαλύτερους πελάτες αλλά επί του παρόντος διαπιστώνουμε ότι οι οργανισμοί μεσαίου μεγέθους υιοθετούν αυτές τις προσεγγίσεις γρηγορότερα από ότι άλλες κατηγορίες οργανισμών.

Τελικά όμως, οι μεγαλύτεροι οργανισμοί θα συνειδητοποιήσουν το δυναμικό μείωσης του κόστους, την ευκολία και τις ολοκληρωμένες εφαρμογές που είναι διαθέσιμες και έτσι θα εξοικειωθούν με αυτή την προσέγγιση των επιχειρηματικών διαδικασιών. Αυτό είναι σίγουρα και το μέλλον της Τεχνολογίας της Πληροφορικής."

6.10. Ο όμιλος S.S.I. προσφέρει λύσεις για τη βελτίωση τη απόδοσης

Εισαγωγή

Ο Όμιλος S.S.I., Inc., είναι μία εθνικής εμβέλειας, πολυμορφική εταιρεία τεχνολογίας πληροφορικής η οποία ιδρύθηκε το 1986. Η εταιρεία είναι ηγετική στο χώρο της τεχνολογίας διαχείρισης αιτήσεων, πλατφόρμων Ηλεκτρονικής Ανταλλαγής Δεδομένων (E.D.I.), δικτύωσης, και τώρα στο χώρο παροχής υπηρεσιών εφαρμογών. Η εταιρεία επί του παρόντος έχει 1200 πελάτες σε όλη τη χώρα και επεξεργάζεται σχεδόν 48 εκατομμύρια συναλλαγές αιτήσεων σε θέματα υγειονομικής περίθαλψης δια μέσου του συστήματος εκκαθάρισης της S.S.I.

Εν όψει των ολοένα και αυξανόμενων πιέσεων του ανταγωνισμού και της ανάγκης μείωσης των εξόδων, οι οργανισμοί υγειονομικής περίθαλψης αναζητούν νέους και διαφορετικούς τρόπους βελτίωσης της απόδοσης και μείωσης των οικονομικών κινδύνων. Η προφανής επιλογή για τους περισσότερους είναι η εκμετάλλευση της ισχύος που προσφέρει η τεχνολογία της πληροφορικής με διάφορους τρόπους, σε εφαρμογές της σε θέματα διοικητικών διαδικασιών, υπηρεσιών πελατών και λήψης αποφάσεων.

Ίσως αυτό να μην είναι πουθενά αλλού τόσο έκδηλο όσο στο χώρο επεξεργασίας αιτήσεων. Με αυτή την λειτουργία αυτή να γίνεται ολοένα και πιο σύνθετη, οι οργανισμοί παίρνουν περισσότερα οικονομικά ρίσκα καθώς έρχονται αντιμέτωποι με νέα έντυπα πληρωμής, νέους κανονισμούς, νέα μεθοδολογία υποβολής και χαμηλότερη απόδοση. Σε μία προσπάθεια εξομάλυνσης και απλοποίησης αναζητούν νέους τρόπους βελτίωσης της απόδοσης και της συνδεσιμότητας. Για την επίτευξη αυτών των σημαντικών στόχων πολλοί ηγετικοί στο χώρο της υγειονομικής περίθαλψης οργανισμοί απευθύνονται στον Όμιλο S.S.I., Inc. Ο Όμιλος S.S.I., ο οποίος ιδρύθηκε το 1986, αρχικά επικεντρώθηκε στην τεχνολογία διαχείρισης αιτήσεων, στις πλατφόρμες Ηλεκτρονικής Ανταλλαγής Δεδομένων (E.D.I.) και στη διαδικτύωση. Σύντομα έγινε μία από τις μεγαλύτερες εταιρείες επεξεργασίας αιτήσεων υγειονομικής περίθαλψης της χώρας, η οποία χειρίζεται ετησίως – μόνο μέσω του συστήματος εκκαθάρισης της SSI - εκατομμύρια συναλλαγών συνολικής αξίας άνω των 36 δισεκατομμυρίων δολαρίων. Υπολογίζεται ότι οι

υπηρεσίες που χρησιμοποιούν την τεχνολογία κόμβων (H.U.B.) Επεξεργασίας της S.S.I. αποστέλλουν πάνω από το διπλάσιο αυτού του ποσού απευθείας στους ασφαλιστές.

Η εταιρεία προσφέρει μεγάλη ποικιλία υπηρεσιών και τεχνολογιών στους ασφαλιστές και τις υπηρεσίες εξυπηρέτησης στο χώρο επεξεργασίας αιτήσεων Ηλεκτρονικής Ανταλλαγής Δεδομένων (E.D.I.), διαχείρισης συμβολαίων /περιπτώσεων /εγγράφων και αποζημιώσεων ασφαλειών υγείας υπαλλήλων /εργασίας και εργατών. Ακόμα, η εταιρεία προσφέρει επικύρωση καταλληλότητας και συμμόρφωσης με την Medicare, οπτική αποθήκευση ως κεντρικό αρχείο και επικύρωση περίθαλψης. Ο στόχος που έχει θέσει η εταιρεία είναι η δημιουργία και εφαρμογή περισσότερο αποτελεσματικών εργαλείων τα οποία να χρησιμοποιούνται από λιγότερους. Μέρος αυτού είναι ένα σύστημα το οποίο επεξεργάζεται αιτήσεις έτσι ώστε να εξασφαλίζεται η υψηλότερη δυνατή πιθανότητα να εξοφλούνται με την πρώτη.

Καθώς το διαδίκτυο επεκτείνει την ηλεκτρονική του εμβέλεια, η εταιρεία διαπίστωσε ότι υπάρχουν πολλοί τρόποι να βοηθηθούν οι οργανισμοί υγειονομικής περίθαλψης ώστε να αυξήσουν την απόδοσή τους. Ο Bobby Smith, Πρόεδρος του Διοικητικού Συμβουλίου (C.E.O.) του Ομίλου S.S.I. δηλώνει: "Η μετάδοση αιτήσεων μέσω διαδικτύου και η Νομοθετική Πράξη Ρύθμισης Μεταφοράς & Αναφοράς Ασφαλειών Υγείας (H.I.P.A.A.) θα ωθήσουν τη βιομηχανία προς την τυποποίηση, κάτι που θα εξομαλύνει πολλές από αυτές τις διαδικασίες, προσφέροντας τελικά απόδοση η οποία δεν ήταν διαθέσιμη στο παρελθόν. Έχουμε δημιουργήσει πολλές εναλλακτικές επιλογές εν όψει της αυξημένης χρήσης του Διαδικτύου. Ο Όμιλος S.S.I. προσφέρει τις εφαρμογές επεξεργασίας αιτήσεων ως εταιρεία διαδικτυακών υπηρεσιών.

"Αυτό αποτελεί μεγάλη βοήθεια για τους οργανισμούς ώστε να αποκτήσουν την αποδοτικότητα εκείνη που χρειάζονται χωρίς το πρόσθετο κόστος αγοράς λογισμικού και εξοπλισμού. Στην πραγματικότητα το κόστος αυτής της προσέγγισης είναι μηδαμινό."

Όσον αφορά μεγαλύτερες εταιρείες οι οποίες διαθέτουν ήδη υποδομή, η S.S.I. μπορεί να προσφέρει επιλογές που κάνουν χρήση αυτών των υποδομών, καθώς επίσης και την απαραίτητη τεχνική γνώση η οποία μπορεί να απαιτείται. "Μπορούμε να τους εγκαταστήσουμε και να τους δώσουμε τη δυνατότητα να θέσουν σε εφαρμογή το δικό τους σύστημα εκκαθάρισης αιτήσεων, κάτι που διευκολύνει την άμεση προώθηση των αιτήσεων στον καταβάλλοντα," δηλώνει ο Smith.

Τα Οφέλη της Νομοθετικής Πράξης Ρύθμισης Μεταφοράς & Αναφοράς Ασφαλειών Υγείας (HIPAA)

Ο Smith ισχυρίζεται ότι, αν και πολλές εταιρείες ανησυχούν αναφορικά με τους κανονισμούς που προτείνει η H.I.P.A.A., εν τούτοις οι χρήστες θα έχουν περισσότερες πληροφορίες στη διάθεσή τους. Θα είναι διαθέσιμες

περισσότερες πληροφορίες σε θέματα δικαιοδοσίας, επικυρώσεων αναφορών, εξουσιοδοτήσεων, καταστάσεων αιτήσεων, επισυνάψεων αιτήσεων, πληρωμών και εμβασμάτων. Κάτι, προσθέτει, το οποίο θα επιφέρει σημαντική αύξηση της απόδοσης.

Μέσω του Σετ Ηλεκτρονικού Εμπορίου "Click On" της εταιρείας, οι πελάτες και οι εταιρείες παροχής υπηρεσιών έχουν τη δυνατότητα να αποκτήσουν ένα πλήρες σετ εφαρμογών βελτίωσης, αυτοματοποίησης της διαχείρισης εγγράφων και της ροής πληροφοριών. Με την πρόσθετη επιλογή της συμβατής με την Νομοθετική Πράξη H.P.A.A. ηλεκτρονικής υπογραφής, το σύστημα μεταβάλλεται σε μία οικονομική λύση μείωσης της γραφειοκρατίας η οποία είναι παράγωγο των συνηθισμένων επιχειρησιακών δραστηριοτήτων. Μία άλλη επιλογή είναι η Μονάδα Σύνδεσης "Click On". Με την επιλογή αυτή τα δεδομένα μπορούν να ληφθούν από οποιαδήποτε πηγή και στη συνέχεια να αναδιαμορφωθούν και να μεταφερθούν αυτόματα σε διάφορα συστήματα. Στη συνέχεια οι εταιρείες παροχής υπηρεσιών μπορούν να μετατρέψουν τα δεδομένα που προέρχονται από οποιοδήποτε εκ των συστημάτων τους σε συναλλαγές σύμφωνες με την H.I.P.A.A.

Τελικά, στόχος της ηλεκτρονικής επεξεργασίας είναι η αύξηση της απόδοσης και η μείωση του κόστους, εξηγεί ο Smith. "Πιστεύουμε ότι βρισκόμαστε στην αιχμή της τεχνολογίας επεξεργασίας αιτήσεων μέσω διαδικτύου και εξελίσσουμε εργαλεία τα οποία θα συμπληρώσουν την διαθέσιμη τεχνολογία και τα ευρέως διαδεδομένα συστήματα."

6.11. Το νοσοκομείο Sherman Ανταποκρίνεται στην πρόκληση του διαδικτύου με το πρόγραμμα RESPOND της Master Chart.

Εισαγωγή

Η Master Chart Inc., με έδρα το Bannockburn του Ιλλινόις είναι μία ταχύτατα αναπτυσσόμενη εταιρεία τεχνολογίας στην αγορά υγειονομικής περίθαλψης, η οποία επικεντρώνει τις δραστηριότητές της στη βελτίωση της κλινικής παραγωγικότητας μέσω αποτελεσματικότερης διαχείρισης των κλινικών δεδομένων. Μεταξύ των λύσεων της Master Chart συμπεριλαμβάνονται τα ηλεκτρονικά ιατρικά αρχεία, η μεταγραφή και παράδοση εγγράφων, η ηλεκτρονική υπογραφή, ή κινητή υπαγόρευση και η τεχνολογία ενοποίησης. Όλα τα προϊόντα της αναπτύσσονται για χρήση με την τεχνολογία Back Office της Microsoft, συμπεριλαμβανομένων Διακομιστών σε Windows NT και S.Q.L.

Η διάθεση της κλινικής πληροφορίας στον γιατρό την κατάλληλη στιγμή είναι κρίσιμης σημασίας για την υποστήριξη της λήψης αποφάσεων που οδηγεί σε καλύτερη παροχή υγειονομικής φροντίδας. Για πολλούς γιατρούς όμως, η πρόσβαση στις πληροφορίες, ακόμα και όταν αυτές υπάρχουν, είναι μία πρόκληση.

Για την αντιμετώπιση αυτής της πρόκλησης και την παροχή μίας διαδικτυακής λύσης το Νοσοκομείο Sherman απευθύνθηκε στη Master Chart. Το νοσοκομείο αυτό με έδρα το Σικάγο το οποίο διαθέτει 275 κλίνες, χρειαζόταν μία λύση η οποία θα παρείχε πληροφορίες στους γιατρούς, ανεξαρτήτως της θέσης τους ή της ώρας της ημέρας. Με τη λύση Ηλεκτρονικών Ιατρικών Αρχείων (E.M.R.) Health Frame και με τη Διαδικτυακή συνιστώσα του "RESPOND", οι γιατροί του Νοσοκομείου Sherman έχουν πλέον τη δυνατότητα πρόσβασης σε κλινικές πληροφορίες μέσω μίας ασφαλούς διαδικτυακής σύνδεσης, οπουδήποτε και αν βρίσκονται, οποτεδήποτε.

Ο Steve Chapman, αντιπρόεδρος και υπεύθυνος πληροφοριών του Νοσοκομείου Sherman, δήλωσε: "Μία σημαντική ομάδα γιατρών μας συνέβαλλε στη διαδικασία επιλογής, αξιολογώντας διάφορες εταιρείες εξοπλισμού και προωθώντας τα διάφορα οφέλη ενός ιατρικού ηλεκτρονικού αρχείου. Το σύστημα αυτό τους ανήκει και μας καθοδηγούν εκεί όπου χρειάζεται να πάνε. Αυτή είναι εξάλλου και η πραγματική απόδειξη, ότι δηλαδή οι ίδιοι οι γιατροί αναγνωρίζουν την αξία αυτού του συστήματος."

Το Νοσοκομείο Sherman Σχεδιάζει να Διευρύνει το Σύστημα

Το Νοσοκομείο Sherman ξεκίνησε να χρησιμοποιεί το σύστημα EMR της Master Chart τον Ιούνιο του 1999, για την αποθήκευση κλινικών αποτελεσμάτων και καταγεγραμμένων αναφορών. Η εφαρμογή του συστήματος από το Νοσοκομείο Sherman πήρε μόλις πέντε μήνες. Οι γιατροί έχουν τη δυνατότητα να επεξεργάζονται και να υπογράφουν αναφορές με ηλεκτρονικό τρόπο καθώς επίσης και να αναλύουν τρέχοντα και παλαιότερα εργαστηριακά αποτελέσματα. Η διαδικτυακή συνιστώσα του Health Frame, RESPOND επιτρέπει στους φυσικούς να έχουν πρόσβαση σε όλα τα δεδομένα από απόσταση από οποιοδήποτε ηλεκτρονικό υπολογιστή με σύνδεση Διαδικτύου.

"Η διαδικτυακή πρόσβαση του συστήματος θα αποτελέσει μεγάλη βοήθεια για τους γιατρούς μας όταν εξασκούν τα καθήκοντά τους σε περισσότερα από ένα σημεία, ή όταν ταξιδεύουν" δηλώνει ο Chapman.

Το Νοσοκομείο Chapman σχεδιάζει μέσα στα επόμενα δύο χρόνια να επεκτείνει τη χρήση του συστήματος Health Frame, συμπεριλαμβάνοντας τη δυνατότητα παραγγελίας φαρμάκων, την παροχή στοιχείων που αφορούν αλλεργίες, ζωτικά όργανα, υγρά, καρδιογραφήματα και ακτινογραφίες. Επίσης, οι γιατροί θα μπορούν να έχουν πρόσβαση σε στοιχεία που αφορούν αλλεργίες ασθενών, ενώ υπάρχουν σχέδια για να συμπεριληφθούν μέχρι το τέλος του έτους και φαρμακολογικά στοιχεία. Η αποθήκευση ακτινογραφιών θα ξεκινήσει μόλις το Νοσοκομείο Sherman εφαρμόσει σύστημα αρχει-

οθέτησης εικόνων, κάτι που θα γίνει εντός του επόμενου έτους. Όλα αυτά θα είναι προσβάσιμα μέσω της συνιστώσας RESPOND του Health Frame.

Ο Αρθρωτός Σχεδιασμός Αναπτύσσεται με την Οργάνωση

Το Health Frame είναι το ισχυρό επιχειρησιακό σύστημα EMR της Master Chart το οποίο βοηθά τους γιατρούς και τους διαχειριστές να ανταποκριθούν στην πρόκληση παροχής υγειονομικής φροντίδας υψηλής ποιότητας και μικρού κόστους. Ο αρθρωτός σχεδιασμός του Health Frame επιτρέπει στους χρήστες να αναπτύξουν το σύστημα όπως εκείνοι επιθυμούν, επιλέγοντας τις μονάδες εκείνες που ανταποκρίνονται καλύτερα στις ανάγκες του οργανισμού τους. Ακόμα, το Health Frame προστατεύει την τρέχουσα επένδυση τεχνολογίας πληροφορικής ενός οργανισμού και διασυνδέεται εύκολα με τα ήδη εγκατεστημένα συστήματα για την απόκτηση και διαχείριση σημαντικών πληροφοριών των ασθενών.

"Επιλέξαμε την Master Chart λόγω του ιστορικού των επιτευγμάτων της" εξηγεί ο Chapman. "Η Master Chart έχει εγκαταστήσει και διατηρήσει με επιτυχία λειτουργικά συστήματα τα οποία δέχονται μεγάλες ποσότητες δεδομένων - 30 Gigabytes ή περισσότερο - και τα οποία εξυπηρετούν 500 χρήστες – γιατρούς σε καθημερινή βάση. Αυτό είναι κάτι που λίγες εταιρείες μπορούν να καταφέρουν. Ακόμα, επικεντρώνει τις προσπάθειές της στον τρόπο με τον οποίο η τεχνολογία μπορεί να ωφελήσει τους γιατρούς και να βελτιώσει την διαδικασία υγειονομικής περίθαλψης, κάτι που είναι αυτό ακριβώς που επιθυμεί και το Νοσοκομείο Sherman."

Το Health Frame λειτουργεί με τον τρόπο με τον οποίο εργάζονται και οι γιατροί. Το περιβάλλον γραφικών του αποτελεί ένα απλό, διαισθητικό εργαλείο διαχείρισης κλινικών πληροφοριών. Οι πολλαπλοί τρόποι απεικόνισης (επεισοδιακοί, χρονολογικοί ή μακροχρόνιοι) διευκολύνουν την εξέταση των συνοπτικών πληροφοριών ή την ανάλυση λεπτομερών δεδομένων. Δίνοντας στους γιατρούς τον έλεγχο των δεδομένων των ασθενών, το Health Frame υποστηρίζει τη λήψη των κλινικών αποφάσεων και βελτιώνει την επικοινωνία μεταξύ των μελών της ομάδας περίθαλψης, ενσωματώνοντας εργαλεία όπως είναι το ηλεκτρονικό ταχυδρομείο, τα ηλεκτρονικά υπομνήματα και η ηλεκτρονική σελιδοποίηση.

Επίσης, το Health Frame αυτοματοποιεί πολλές από τις συνηθισμένες και βαρετές εργασίες που είναι υποχρεωμένοι να πραγματοποιήσουν οι γιατροί. Για παράδειγμα, το Health Frame επιτρέπει στους γιατρούς να δημιουργούν, να επεξεργάζονται και να πιστοποιούν με ηλεκτρονικό τρόπο έγγραφα. Μέσω της χρήσης του "ηλεκτρονικού πλαισίου εισαγωγής στοιχείων" οι γιατροί μπορούν να γρήγορα και εύκολα να ικανοποιήσουν και άλλες ανάγκες συμπλήρωσης ιατρικών αρχείων.

Μεταξύ άλλων μονάδων του Health Frame συμπεριλαμβάνονται:

- Διαχείριση απογραφής
- Ηλεκτρονικής υπογραφής

- Δημιουργία εγγράφων
- Πρακτικές φορητές συσκευές

6.12. Τα κλινικά εργαστηριακά αποτελέσματα στον πυρήνα του.

Daily Apple.com

Επαναστατικές Υπηρεσίες Προσφέρουν Νέες Δυνατότητες στους Καταναλωτές

Εισαγωγή

Η Caresoft Inc., προσφέρει ένα διαδικτυακό κέντρο πληροφοριών το οποίο συγκεντρώνει και ενσωματώνει δεδομένα συγκεκριμένων ασθενών από τα συνεργαζόμενα δίκτυα, συμπεριλαμβανομένων αυτών των εργαστηρίων, των φαρμακείων και των καταναλωτών. Ως κέντρο πληροφοριών υγειονομικής περίθαλψης, η βάση δεδομένων της Caresoft προσφέρει συνδεσιμότητα σε εταιρείες από ολόκληρο τον κλάδο της βιομηχανίας της περίθαλψης και προσφέρει στα συνεργαζόμενα δίκτυα μία πλήρη πηγή πληροφοριών συγκεκριμένων ασθενών, επικοινωνία και ευκαιρίες ηλεκτρονικού εμπορίου.

Η Caresoft διατηρεί την TheDailyApple.com, μία ιστοσελίδα καταναλωτών όπου κάθε μέλος έχει μία προσωπική και ιδιαίτερα ασφαλή σελίδα με πρόσβαση στα δικά του /της κλινικά, φαρμακευτικά και ιατρικά δεδομένα.

Η TheDailyApple.com είναι η πρώτη ιστοσελίδα στο χώρο της περίθαλψης η οποία συνδέει τους καταναλωτές με τα κλινικά εργαστηριακά τους δεδομένα και παρέχει διαδραστικά προγράμματα υγείας τα οποία επικεντρώνονται σε κοινές ασθένειες και καταστάσεις, σε προσωπικό περιεχόμενο, σε ολοκληρωμένα ιατρικά αρχεία και σε υπηρεσίες υποστήριξης. Η Caresoft είναι μία ιδιωτική εταιρεία με έδρα το Sunnyvale της Καλιφόρνια.

Το διαδίκτυο έχει δημιουργήσει μία πληθώρα νέων και εύκολων τρόπων πρόσβασης πληροφοριών υγείας ή αγοράς προϊόντων υγείας από τους καταναλωτές. Οι περιοχές όμως του διαδικτύου οι οποίες προσέφεραν περιεχόμενο, συναλλαγές ή ακόμα και αναφορά προσωπικών ιατρικών αρχείων σύντομα τροποποιήθηκαν, καθώς μέχρι τώρα προσέφεραν ελάχιστα ή και τίποτα που να τις κάνει να διαφέρουν μεταξύ των καταναλωτών ή της φαρμακευτικής βιομηχανίας, που είναι και οι βασικές πηγές εσόδων πολλών ιστοσελίδων.

Ενώ οι ιστοσελίδες προσφέρουν κυριολεκτικά χιλιάδες επιλογών, διαθέτουν ελάχιστη ή και καθόλου πρωτοτυπία. Μάλιστα, καθώς η προσοχή των καταναλωτών μειώνεται, οι παραδοσιακές μέθοδοι προώθησης μέσω διαδικτύου θα αποτελούν όλο και μεγαλύτερη πρόκληση για τους συναλλασσόμενους στο φαρμακευτικό χώρο οι οποίοι αναζητούν πραγματικές λύσεις για τη δημιουργία καλύτερων σχέσεων με τους πελάτες. Οι συναλλασσόμενοι στο φαρμακευτικό χώρο αναζητούν νέες και καινοτομικές λύσεις για να προσεγγίσουν το κοινό τους, λύσεις οι οποίες απαιτούν ακρίβεια λέιζερ.

Όλα Αυτά Αφορούν τους Ασθενείς-Καταναλωτές

Στο επίκεντρο της επιτυχίας της TheDailyApple.com βρίσκεται η παροχή πληροφοριών ακριβείας, οι οποίες σχετίζονται με τα ενδιαφέροντα κάθε μέλους. Η εμπειρία της Caresoft έδειξε ότι η παροχή πραγματικών δεδομένων που αφορούν την υγεία ενός ατόμου, σε συνδυασμό με την παροχή άμεσα σχετικών πληροφοριών και υπηρεσιών έχει πολύ μεγαλύτερη αξία – και καθιστά τις ιστοσελίδες πολύ πιο ελκυστικές – από ότι απλώς η ανάγνωση περιεχομένου που μπορεί να βρεθεί στις περισσότερες ιστοσελίδες υγειονομικής περίθαλψης.

Η Caresoft εισάγει μία νέα υπηρεσία η οποία, για πρώτη φορά, επιτρέπει στους καταναλωτές να έχουν πρόσβαση στα αποτελέσματα των εργαστηριακών κλινικών αποτελεσμάτων τους μέσω διαδικτύου. Η υπηρεσία εργαστηριακών αποτελεσμάτων είναι έτσι σχεδιασμένη ώστε να εκπαιδεύει τους καταναλωτές στα θέματα της υγείας τους και να τους προσφέρει καλύτερη κατανόηση των εργαστηριακών αποτελεσμάτων, δίνοντάς τους έτσι τη δυνατότητα να αξιοποιούν στο μέγιστο το χρόνο τους κατά τη διάρκεια των τακτικών επισκέψεων τους στο γιατρό. Τα αποτελέσματα χορηγούνται από την Quest Diagnostics Inv., την μεγαλύτερη υπηρεσία παροχής...

Επίσης, η ιστοσελίδα προσφέρει 20 Κέντρα Φροντίδας, καλύπτοντας τις πιο κοινές ασθένειες, καταστάσεις και προβληματισμούς των διασυνδεδεμένων καταναλωτών. Στις προσωπικές υγειονομικές υπηρεσίες οι οποίες συμπληρώνουν τα Κέντρα Φροντίδας, συμπεριλαμβάνονται προσωπικά αρχεία κατάστασης υγείας, εργαστηριακά αποτελέσματα, υπενθυμίσεις ραντεβού και λήψης φαρμακευτικής αγωγής, μία ιατρική και φαρμακευτική

βιβλιοθήκη, τα τελευταία νέα σε θέματα υγείας και έρευνας, ομάδες συζήτησης, αγορές και δυνατότητα αποστολής φαξ ή εκτύπωσης αρχείου υγείας. Όλα αυτά συνθέτουν μία ιδιαίτερα χρήσιμη υπηρεσία για τους καταναλωτές αλλά και για τους επιχειρηματικούς συνεργάτες.

Ο Κόμβος Πληροφοριών Προσφέρει Νέες Ευκαιρίες

Η TheDailyApple.com ως πληροφοριακός κόμβος επιτρέπει στις φαρμακευτικές εταιρείες να δημιουργήσουν σχέσεις με ιδιαίτερα ικανούς και δραστήριους καταναλωτές. Η ιστοσελίδα αυτή βελτιστοποιεί τη διαδικασία διαχείρισης των σχέσεων των πελατών προσφέροντας προγράμματα υγείας τα οποία είναι συναφή με τα διάφορα προϊόντα, καθώς και πραγματικά δεδομένα που αφορούν κάθε καταναλωτή.

Ο Singh λέει ότι το πλήρες πακέτο διαδικτυακών υπηρεσιών, Πληροφοριών και προϊόντων της Caresoft την διαχωρίζει από τις άλλες ιστοσελίδες με θέματα υγείας που απευθύνονται σε καταναλωτές και θέτει μία στερεή πλατφόρμα διαχείρισης των πελατειακών σχέσεων. "Οι περισσότερες από τις κορυφαίες ιστοσελίδες που καλύπτουν θέματα υγείας ουσιαστικά βασίζονται στο περιεχόμενο για να προσελκύσουν τους καταναλωτές" δηλώνει ο Singh. "Αυτό όμως αποτελεί μόνο μία καμπάνια ενημέρωσης. Δεν αποτελεί αγορά και δεν επιφέρει αλλαγή συμπεριφοράς. Η TheDailyApple.com εμπλέκει τους χρήστες κατά τέτοιο τρόπο ώστε βοηθά στη διαμόρφωση του τρόπου με τον οποίο σκέφτονται και ενεργούν στα θέματα υγείας που τους προβληματίζουν."

Ακόμα, υπάρχουν και άλλοι οργανισμοί που επιζητούν την επέκτασή τους στο χώρο της ηλεκτρονικής υγειονομικής φροντίδας και απευθύνονται στην TheDailyApple.com για τη βελτίωση των σχέσεών τους με τους πελάτες. "Η ιστοσελίδα λειτουργεί σε συνεργασία με προγράμματα υγείας, γιατρούς και φαρμακευτικές, έτσι ώστε να καθίσταται δυνατή η παροχή υπηρεσιών και προγραμμάτων πραγματικής αξίας σε μέλη," λέει ο Singh. Με το συνδυασμό στοιχείων συγκεκριμένων ασθενών και συγκεκριμένου ιατρικού περιεχομένου μέσω πανίσχυρων εργαλείων, η Caresoft προσφέρει ασύγκριτες υπηρεσίες στους συνεργάτες της.

"Αν πρόκειται να αποδεσμευτεί το τεράστιο δυναμικό της ηλεκτρονικής περίθαλψης, αυτό δεν πρόκειται να γίνει μέσω των διαφημίσεων του διαδικτύου. Σημαντικός παράγοντας σε αυτό είναι η ενσωμάτωση κρίσιμων πληροφοριών ασθενών από διάφορους οργανισμούς υγείας με σχετικές πληροφορίες και υπηρεσίες που επιζητούν οι ασθενείς και αυτό ακριβώς είναι που προσφέρει και η Caresoft."

6.13. Διαδικτυωμένοι γιατροί εθίζονται στο πρόγραμμα σύνταξης συνταγών Axolotl.

Εισαγωγή

Ο Οργανισμός Axolotl παρέχει λύσεις ιατρικής επικοινωνίας μεταξύ ανεξάρτητων γιατρών και των συνεργατών τους σε θέματα υγειονομικής φροντίδας. Το σετ προϊόντων της Axolotl, Elysium χρησιμοποιεί το διαδίκτυο, το ηλεκτρονικό ταχυδρομείο και την πανίσχυρη τεχνολογία αυτοματοποίησης για να διασυνδέσει τους γιατρούς και να βελτιώσει την ιατρική φροντίδα των ασθενών και την απόδοση των γραφειοκρατικών εργασιών. Το Elysium με την πρότυπη ανοικτή αρχιτεκτονική τους διασυνδέεται με τα ήδη υπάρχοντα συστήματα νοσοκομείων, εργαστηρίων και άλλων υπηρεσιών και παρέχει ηλεκτρονική διανομή αποτελεσμάτων, εξουσιοδοτήσεις και αναφορές, υποστήριξη διαδικασιών, σύνταξη συνταγών και διαχείριση συνεχόμενων ιατρικών συνταγών, εργαστηριακές παραγγελίες και άλλες κλινικές συνιστώσες αυτοματοποίησης. Οι λύσεις κλινικής επικοινωνίας διασυνδέουν χιλιάδες γιατρούς και υπηρεσίες εξυπηρέτησης σε ολόκληρη τη χώρα.

"Είμαι πλέον εθισμένος" δηλώνει ο Δόκτωρ Arnold Leff "και ούτε περνά από το μυαλό μου να κάνω πίσω." Ο οικογενειακός γιατρός Δόκτωρ Leff, καθώς και οι συνεργάτες του στον Όμιλο Γιατρών, έναν Ανεξάρτητο Ιατρικό Οργανισμό (I.P.A.) της Santa Cruz της Καλιφόρνια έχουν γίνει πράγματι άπληστοι χρήστες του Συστήματος Έκδοσης Συνταγών της Axolotl.

Ο Δόκτωρ Leff ήταν ήδη ένας ικανοποιημένος πελάτης. Η εξάσκηση των καθηκόντων του ως οικογενειακού γιατρού επί μακρόν βασίζονταν στο διαδικτυακό και ενδοδικτυακό σύστημα Elysium της Axolotl για εργασίες όπως η έκδοση αναφορών, εξουσιοδοτήσεις, παροχή ραδιολογικών και εργαστηριακών εξετάσεων και πλήρες ηλεκτρονικό ταχυδρομείο. Έτσι, όταν αναζήτησε ένα ευκολότερο τρόπο διαχείρισης των συνταγών, σύντομα έγινε φανατικός χρήστης του Συστήματος Έκδοσης Συνταγών Elysium.

Καθώς ο Δόκτωρ Leff αναζητούσε πάντα την ποιότητα, οι στόχοι του, όπως λέει, ήταν πάντα δύο. "Ο ένας ήταν η αποφυγή της γραφειοκρατίας – όσο λιγότερα έγγραφα εμπλέκονται τόσο το καλύτερο," θυμάται". Ο δεύτερος ήταν κατά κάποιο τρόπο και ο πιο σημαντικός: Η βελτίωση της ποιότητας εξασφαλίζοντας την αρχειοθέτηση όλων των συνταγών και τελικά η συμμετοχή και των 200 γιατρών του I.P.A. στο σύστημα Έκδοσης Συνταγών Elysium. Με αυτό τον τρόπο μπορούμε να αποφεύγουμε αντενδείξεις και αρνητικές αλληλεπιδράσεις και να διατηρούμε μία σταθερή λίστα όλων των φαρμάκων που λαμβάνει κάθε ασθενής – την οποία να μοιράζονται όλοι οι θεράποντες γιατροί τους, καθώς και το προσωπικό στα έκτατα περιστατικά και τα νοσοκομεία."

Ο γιατρός πλέον τώρα έχοντας συνηθίσει τις λύσεις της Axolotl, διαπιστώνει ότι ο διαδικτυακός κόσμος είναι πολύ πιο πρακτικός. Η έκδοση νέων συνταγών και η απάντηση σε αιτήσεις ανανέωσής τους, πράγματα που μπορούν να γίνουν μέσω του ηλεκτρονικού ταχυδρομείου ή μέσω φαξ στα συμβαλλόμενα φαρμακεία, είναι μόλις η κορυφή του παγόβουνου για το Σύστημα Έκδοσης Συνταγών Elysium.

Ο Δόκτωρ Leff κρίνει ότι "η πρόσβαση στους ηλεκτρονικούς υπολογιστές είναι πολύ ευκολότερη πλέον," αναφέροντας την αποφυγή αρνητικών φαρμακευτικών επιδράσεων ως σημαντικό παράγοντα. "Οι πληροφορίες που αφορούν αλληλεπιδράσεις δεν ανευρίσκονται εύκολα σε ένα βιβλίο όπως το Βιβλίο Αναφοράς του Γιατρού. Με τον νέο τρόπο μπορούμε απλώς να τσεκάρουμε τα δύο φάρμακα τα οποία μας ενδιαφέρουν και ο υπολογιστής θα κάνει τα υπόλοιπα.." Ο Δόκτωρ Leff χρησιμοποιεί το πλήρες, προσβάσιμο Σύστημα Έκδοσης Συνταγών για να ελέγχει τυχόν αλληλεπιδράσεις φαρμάκων σε καθημερινή βάση.

Ένα απλό κλικ στον δείκτη ειδοποίησης της οθόνης διαλόγου αρκεί για να κοινοποιηθεί το πρόβλημα στους χρήστες - ο Δόκτωρ Leff είχε μερικές τέτοιες περιπτώσεις. "Σε κάθε περίπτωση, δεν ανησυχούσα πραγματικά για την αλληλεπίδραση, αλλά χαιρόμουν που το Πρόγραμμα Έκδοσης Συνταγών ανησυχούσε για μένα," λέει γελώντας.

Είναι εύκολο να εξαρτηθεί κανείς από ένα εργαλείο του διαδικτύου το οποίο είναι τόσο εύχρηστο όσο αυτό εδώ. Για παράδειγμα, το Πρόγραμμα Έκδοσης Συνταγών Elysium βοηθά έξυπνα τον κλινικό γιατρό να συμπληρώσει το έντυπο συνταγών. "Δεν είσαι υποχρεωμένος να συμπληρώνεις ονόματα ή οτιδήποτε άλλο," παρατηρεί ο Δόκτωρ Leff, διότι είναι ήδη προ-συμπληρωμένα. "Η επιλογή ενός φαρμάκου απαιτεί μόνο ένα κλικ. Υπάρχουν προεπιλογές ποσότητας, δοσολογίας και οδηγιών για μία τυπική συνταγή ενός συγκεκριμένου φαρμάκου, κάθε μία εκ των οποίων μπορεί να τροποποιηθεί εύκολα."

Η χρήση χαρτιού στο γραφείο του Δόκτορα Leff είναι μειωμένη. Το γεγονός ότι μπορεί να γράψει μία συνταγή χρησιμοποιώντας το πρόγραμμα Έκδοσης Συνταγών Elysium τόσο γρήγορα όσο θα την έγραφε και με το χέρι, αποτελεί πρόοδο. Καθώς η χρήση χαρτιού μειώνεται, συνεχίζει, μειώνεται επίσης και η πιθανότητα κακής διαχείρισης σημαντικών εγγράφων από τους ασθενείς και τους γιατρούς, όπως είναι οι συνταγές.

Οι γιατροί αγκάλιασαν τα προϊόντα Axolotl Elysium, διότι είναι σχεδιασμένα από γιατρούς και απευθύνονται σε γιατρούς. Ο Δόκτωρ Leff δηλώνει: "Οι γιατροί ωφελούνται πραγματικά από τη χρήση του Προγράμματος Έκδοσης Συνταγών. Όταν δε τα μέλη του προσωπικού υποστήριξης του γιατρού χρησιμοποιούν το σύστημα, το Elysium βελτιώνει ακόμα περισσότερο τις εργασιακές δραστηριότητες του γραφείου."

"Πρόκειται για μία βελτίωση της ποιότητας", καταλήγει με έμφαση. "Η χρήση και μόνο αυτού του συστήματος με οποιονδήποτε τρόπο αποτελεί μία ποιοτική βελτίωση".

ΚΕΦΑΛΑΙΟ ΕΒΔΟΜΟ

ΤΕΧΝΙΚΟ ΜΕΡΟΣ

Εφαρμογή των Τεχνικών Διαδικασιών (ΑΣΦΑΛΕΙΑ-ΕΛΕΓΧΟΣ) σε ένα Νοσοκομειακό Περιβάλλον.

Ο Barney Oliver που είναι επικεφαλής των εργαστηρίων Hewlett-Packard είπε "...η μοναδική διαφορά μεταξύ θεωρίας και πράξης είναι, ότι η πράξη λαμβάνει υπόψη της κάθε θεωρία" .

Στην πτυχιακή αυτή προτίθονται όλες οι συνιστώσες που απαιτούνται για την ασφάλεια και τον έλεγχο ενός νοσοκομειακού πληροφοριακού συστήματος. Αναλύσαμε τις τρείς (3) βασικές προυποθέσεις της ασφάλειας (εμπιστευτικότητα-ακεραιότητα-διαθεσιμότητα) όπου βοηθούν τον χρήστη ιδιαίτερα σε πολύπλοκες εφαρμογές όπως είναι τα νοσοκομειακά πληροφοριακά συστήματα.

Ένα μεγάλο πληροφοριακό έργο ήταν η μηχανογράφηση στον χώρο της υγείας. Από το 1986 ξεκίνησε ένα πιλοτικό έργο μέσω των Μ.Ο.Π της πληροφορικής με 15 Νοσοκομεία. Τα αποτελέσματα για τα πρώτα χρόνια δεν θεωρούνταν ικανοποιητικά στην εφαρμογή τους λόγω της έλλειψης υποδομής των νοσοκομείων καθώς και στις γραφειοκρατικές μεθόδους για την αγορά εξοπλισμού, ώστε να προσαρμοστούν στα νέα δεδομένα. Μεγάλη αργοπορία είχε παρουσιαστεί κυρίως στον σχεδιασμό και την υλοποίηση των υποσυστημάτων.

Για τα διοικητικά θέματα διαχείρησης των Νοσοκομείων υπεύθυνος φορέας είναι το Κ.Η.Υ.Κ.Υ του Υπουργείου Υγείας. Όσο για το σύστημα ασθενών (ιατρικός φάκελος) είχε γίνει ανάθεση απο το 1993 με εξωτερικά **SOFTWARE HOUSES**. Το σύστημα αυτό παραδόθηκε στα τέλη του 1995 όπου άρχισε να λειτουργεί.

Συχνά χρησιμοποιείται το εξωτερικό γραφείο (software house) οπότε το σύστημα ονομάζεται "turn-key-system" δηλαδή σύστημα κατά παραγγελία. Η μέθοδος αυτή χρησιμοποιείται όταν το σύστημα είναι έξω απο τις δυνατότητες του προσωπικού που διαθέτει ο οργανισμός ή σε περιπτώσεις που δεν υπάρχουν έτοιμα πακέτα που να καλύπτουν τις ανάγκες του. Η λύση αυτή είναι λιγότερο δαπανηρή απο την λύση ανάπτυξης του συστήματος εντός του οργανισμού και προβάλλει αναγκαία όταν δεν υπάρχει επάρκεια σε προσωπικό. Σ'αυτήν την περίπτωση ο οργανισμός συμμετέχει με τις ομάδες εργασίας τους, οι οποίες συνεργάζονται με την ανάδοχο κατασκευάστρια εταιρία.

Στο κεφάλαιο αυτό αναλύεται το σύστημα που εφαρμόζεται στο Πανεπιστημιακό Νοσοκομείο "**ΑΡΕΤΑΙΕΙΟ**" όπου λειτουργεί με την μορφή software house. Το πρόγραμμα που εφαρμόζεται στο νοσοκομείο που εξετάζουμε είναι το **HELLIOS** το οποίο έχει σχεδιαστεί και εγκατασταθεί από την

ανάδοχο κατασκευάστρια εταιρία Intrasoft. Στην συνέχεια οι ενότητες που θα εξετασθούν είναι οι:

1. Διαθεσιμότητα μηχανών-Λειτουργικού συστήματος καθώς και ορθότητα δεδομένων.
2. Ρόλοι χρηστών σε νοσοκομειακό πληροφοριακό σύστημα.
3. Προστασία ατόμου απο την επεξεργασία δεδομένων προσωπικού χαρακτήρα. (ΝΟΜΟΣ 2472/97) βλέπε παράρτημα

7.1. Απαιτήσεις διαθεσιμότητας μηχανών και λειτουργικού συστήματος.

Όταν το ιατρικό πληροφοριακό σύστημα διαδραματίζει ένα σημαντικό ρόλο στην διαδικασία της περίθαλψης, όπως όντως συμβαίνει στα περισσότερα Ι.Π.Σ., προκύπτει ανάγκη υψηλής διαθεσιμότητας. Η συνηθισμένη απαίτηση είναι διαθεσιμότητα μεγαλύτερη απο 99.7% ανά πάσα στιγμή. Εκτός απο τη διαθεσιμότητα, ο χρόνος αποκατάστασης των λει-τουργιών μετά απο μια διακοπή είναι σημαντικός. Μπορούμε να διακρίνουμε τρεις καταστάσεις:

- Δυνατότητα απλής επανεκκίνησης, αποκατάστασης μερικών παραμέτρων του συστήματος και ελέγχου των σημαντικών δεδομένωντου συστήματος. Δεν απαιτείται συνήθως χρόνος μεγαλύτερος από δέκα λεπτά.
- Η βάση δεδομένων έχει πάθει βλάβη είτε από δυσλειτουργία του υλικού, είτε από πρόβλημα στο λογισμικό, είτε από ανθρώπινο λάθος. Απαίτηση ανάνηψης απο ασφαλή αντίγραφα και μεταβολές που έχουν καταγραφεί. Δεν απαιτείται χρόνος μεγαλύτερος απο 4-6 ώρες.
- Το υπολογιστικό κέντρο (ή το μεγαλύτερο τμήμα του εξοπλισμού που βρίσκεται εκεί) έχει καταστραφεί απο φυσική αιτία, για παράδειγμα, εξαιτίας μιας μεγάλης πυρκαγιάς. Σε αυτή την περίπτωση απαιτούνται εξωτερικές δυνατότητες τήρησης εφεδρικών αντιγράφων σε ένα κινητό ή μακρινό υπολογιστικό κέντρο. Στην τελευταία περίπτωση πρέπει να είναι διαθέσιμες και δυνατότητες επικοινωνιών των δεδομένων.Παρά το γεγονός ότι τέτοιες καταστροφές συμβαίνουν σπάνια (σπανιότερα απο μια φορά στα πενήντα χρόνια), η διακοπή των υπηρεσιών σε ένα νοσοκομείο δεν πρέπει να διαρκεί περισσότερο απο ένα εικοσιτετράωρο.

Καθώς αυξάνεται η σημασία του ρόλου που διαδραματίζουν τα πληροφοριακά συστήματα στην άμεση περίθαλψη των ασθενών,οι απαιτήσεις θα γίνονται όλο και περισσότερο αυστηρές. Ο κατοπτρισμός (mirroring) της βάσης είναι μια απο τις τχνικές που χρησιμοποιούνται για να μειώσουν το κίνδυνο απώλειας της βάσης. Έπειτα ακολουθεί μια χρονοβόρα ενέργεια ανάνηψης

Η λεγόμενη "ακατάπαυστη λειτουργία" ("non-stop operation") θα έπρεπε να θεωρηθεί ως σοβαρή προοπτική.Εντούτοις,πρέπει να γίνει κατανοητό ότι έτσι δεν προσφέρεται καμιά προστασία κατά των φυσικών καταστροφών,των ανθρώπινων λαθών και των λανθασμένων επανεκδόσεων των υποσυστημάτων λογισμικού. Εν πάση περιπτώσει, τα ακατάπαυστα εργαλεία διευκόλυνσης δεν εμπίπτουν στο λογισμικό της βάσης, εξαιτίαςτης φύσης τους.

Όσο αναφορά το Αρεταίειο Νοσοκομείο υπάρχουν δύο (2) διαδικασίες (manual-cluster) που αφορούν την διαθεσιμότητα των μηχανών και του

λειτουργικού συστήματος. Για την ασφάλεια του συστήματος το τμήμα πληροφορικής διαθέτει δυο (2) μηχανές την κύρια και την εφεδρική.

Κατά την manual διαδικασία στο τέλος των ημερήσιων εργασιών κάνουμε data back up, στην κύρια μηχανή και data restore στην εφεδρική με σκοπό αν κάποια ημέρα δεν ξεκινάει ή πέσει η κύρια μηχανή χωρίς να μπορούμε να την ανακτήσουμε τότε ξεκινάμε με την εφεδρική η οποία καλύπτει τιστρέχουσες ανάγκες των χρηστών μέχρι να αποκατασταθεί η βλάβη στην κύρια μηχανή.

Στην διαδικασία cluster δεν έχουμε μη συχρονισμένα δεδομένα ενώ ο χρόνος που χρειάζεται για να αντικατασταθεί η μηχανή ένα από την δύο είναι ελάχιστος εώς ανύπαρκτος ανάλογα με τον τύπο του cluster. Συμπερασματικά αναφέρουμε ότι η διαθεσιμότητα των μηχανών καθώς και ενός λειτουργικού συστήματος είναι η ιδιότητα του να να εξασφαλίζει:

- Τη **λογική ορθότητα** (correctness), την αξιοπιστία (reliability) και την ανοχή σε σφάλματα (fault tolerance) του υλικού και του λογισμικού του συστήματος,
- Τη **λογική πληρότητα** (completeness) των μηχανισμών εξασφάλισης του υλικού και του λογισμικού,
- Τη **συνοχή** (consistency) των δομών των δεδομένων και την ακρίβεια των αποθηκευμένων δεδομένων.

Η διαθεσιμότητα (availability) ενός Λειτουργικού Συστήματος είναι η ιδιότητα του να εξασφαλίζει στους εξουσιοδοτημένους χρήστες την πρόσβαση στα αντικείμενα του συστήματος που επιθυμούν, με τον αποδοτικότερο τρόπο.

Αυτό σημαίνει ότι το σύστημα πρέπει να λειτουργεί ώστε, όχι μόνο να προστατεύει απο τους μη εξουσιοδοτημένους χρήστες, αλλά να προστατεύει τα δικαιώματα και των εξουσιοδοτημένων χρηστών. Η διαθεσιμότητα ενός λειτουργικού συστήματος είναι συχνά αντιφατική με τις διαδικασίες εξασφάλισής του. Έτσι, αν οι διαδικασίες αυτές εφαρμόζονται συχνά και απαιτούν σημαντικό χρόνο,τότε μειώνεται ο ωφέλιμος χρόνος που διατίθεται στο χρήστη, άρα και η συνολική διαθεσιμότητα του συστήματος.

Η συνύπαρξη των ιδιοτήτων ασφαλείας και διαθεσιμότητας, είναι θέμα ισορροπίας μεταξύ της επιδιωκόμενης φιλικότητας και αξιοπιστίαςενός σχεδιαζόμενου Λειτουργικού Συστήματος.

7.2. Προστασία του ατόμου.

Για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να υπάρχουν κάποια επιθυμητά μέτρα ασφαλείας. Παρακάτω ορίζουμε τις εξής γενικές συνθήκες ασφαλείας:

- Στα προσωπικά στοιχεία ενός ασθενή έχουν προσπέλαση μόνο ο ιατρός και το προσωπικό διαχείρισης. Το προσωπικό διαχείρισης έχει προσπέλαση μόνο σε αυτές τις πληροφορίες, αφού μόνο αυτές ανήκουν στην κατηγορία διαχείρισης.

• Οι νοσηλεύτριες δεν έχουν ποτέ βαθμό εξουσιοδότησης, τέτοιο, ώστε να έχουν προσπέλαση στην ταυτότητα του ασθενή (όνομα, διεύθυνση ή οποιαδήποτε πληροφορία που μπορεί να οδηγήσει σε αποκάλυψη της προσωπικοτητάς του) από το γεγονός αυτό συνεπάγονται τα εξής:

1) Εαν ο ασθενής δεν έχει τις αισθήσεις του, η νοσηλεύτρια ή οποιοδήποτε άλλο άτομο του προσωπικού ιατρικής υποστήριξης δε χρειάζεται να γνωρίζει το όνομα του, ώστε να επικοινωνήσει μαζί του.
2) Εάν ο ασθενής έχει τις αισθήσεις του, τότε είναι ελεύθερος να αποκαλύψει την ταυτοτητά του.

Όμως σε καμιά περίπτωση το προσωπικό ιατρικής υποστήριξης δεν μπορεί να προσπελάσει την ταυτότητα του ασθενή.

• Εν τούτοις, για τα διάσημα πρόσωπα, για το προσωπικό του νοσοκομείου, ή για τα πολύ σημαντικά πρόσωπα η παραπάνω διαδικασίες δεν μπορούν να προστατεύσουν την εμπιστευτικότητα, αφού το ονομά τους είναι ήδη γνωστό. Συνεπώς, γίνεται επικάλυψη πληροφοριών (cover stories) για τις παραπάνω περιπτώσεις, αλλά και για τις ευαίσθητες (sensitive) ασθένειες.
• Επομένως το όνομα του ασθενή και όλα τα προσωπικά του στοιχεία αναγνώρισης πρέπει να είναι γνωστά μόνο στους γιατρούς και τους χρήστες οργάνωσης.
• Μόνο οι ιατροί πρέπει να μπορούν να έχουν ταυτόχρονη προσπέλαση και στα προσωπικά στοιχεία αναγνώρισης και στα ιατρικά στοιχεία
• Οι νοσηλεύτριες μπορούν να προσπελάσουν τα δεδομένα που χρειάζονται, ώστε να εκτελούν τις εργασίες τους. Όμως, δεν επιτρέπεται η προσπέλαση στις πληροφορίες που αφορούν στην εξέλιξη της θεραπευτικής αγωγής.
• Οι ευαισθητες διαγνώσεις (δηλαδή διαγνώσεις για V.I.P άτομα, προσωπικό του νοσοκομείου και διάσημα πρόσωπα) πρέπει να είναι γνωστές μόνο στις ειδικές νοσηλεύτριες.

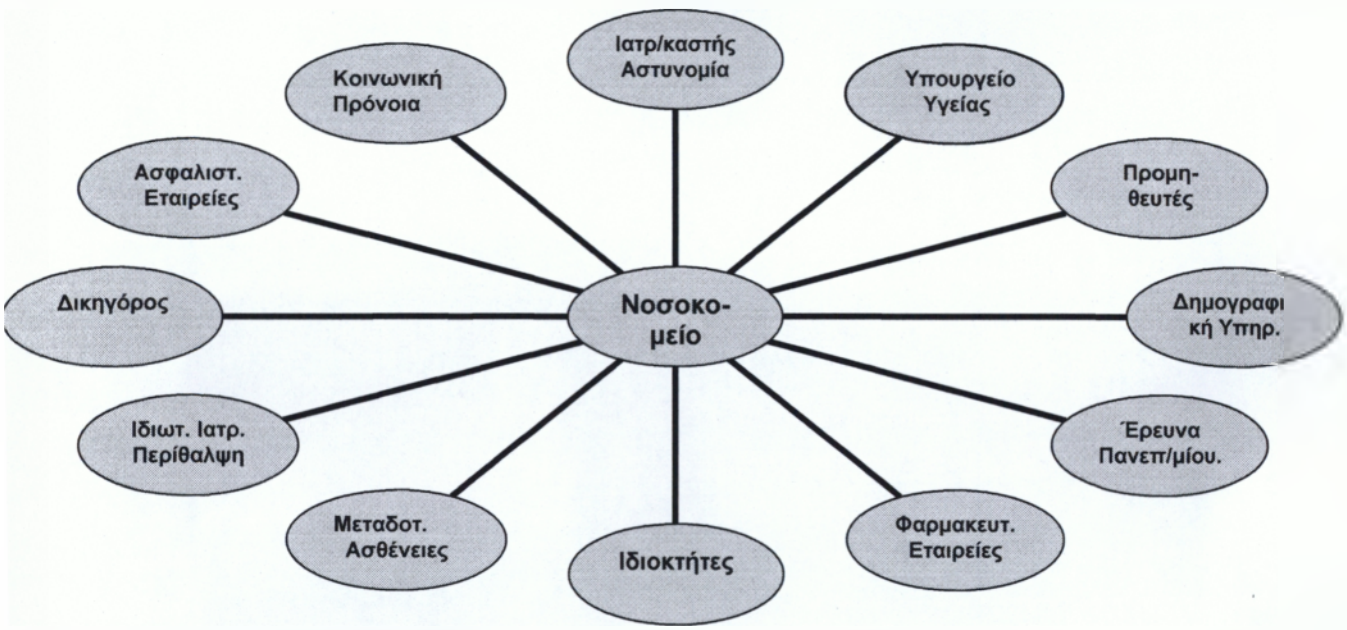
Επίσης απο την φάση αυτή προκύπτει η αναγκαιότητα επιλογής ενός μοντέλου πολιτικής ασφαλείας, εάν βέβαια αυτό υπάρχει. Καμία από τις ήδη υπάρχουσες πολιτικές ασφαλείας δεν μπορεί να υποστηρίξει ολοκληρωτικά την ασφάλεια της πρότυπης εφαρμογής. Όσο αναφορά για την προστασία του ατόμου το κράτος έχει θεσπίσει νόμους και ορίζει διατάξεις για την προστασία του απο την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι οποίες αναφέρονται στον υπ'αριθμό νόμο 2472/97 και οι σχετικές τροποποιήσεις που έχει υποστεί αυτός που παραθέτονται ακολούθως.

7.2.1. Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Ένα πραγματικό πληροφοριακό σύστημα ενός περιβάλλοντος υγείας αλληλεπιδρά σε μεγάλο βαθμό με διάφορα "εξωτερικά συστήματα" (external system), όπως θα μπορούσαμε να τα αποκαλέσουμε (σχήμα.1). Για να διαφυλάξουμε την ασφάλεια όλης της εφαρμογής, η ολοκληρωμένη ανάπτυξη ενός περιβάλλοντος υγείας πρέπει να λαμβάνει υπόψη όλες τις πιθανές αλληλεπιδράσεις, γιατί ένα μεγάλο μέρος των δεδομένων (κάθε κατηγορίας

και ευαισθησίας) μπορεί να διακινείται, όταν αυτά τα συστήματα /οργανισμοί επικοινωνούν.

Συνεπώς, πρέπει να εξασφαλίζεται ότι τα δεδομένα προστατεύονται στον ίδιο βαθμό εντός και εκτός ενός συστήματος, δηλαδή η πολιτική ασφαλείαςτου περιβάλλοντος υγείας πρέπει να καλύπτει όλες τις περιοχές, όπου βρίσκονται ή μεταφέρονται δεδομένα. Αυτό μπορεί να επιτευχθεί, τουλάχιστον, ελέγχοντας την ροή των πληροφοριών που εξέρχονται από το σύστημα και εξασφαλίζοντας, όσο είναι δυνατό, ότι οι πληροφορίες αυτές έχουν τον ίδιο βαθμό ευαισθησίας, όπως και εντός του συστήματος.



Σχήμα:Το ολοκληρωμένο περιβάλλον ιατρικής περίθαλψης

Ακόμη, όμως στην περίπτωση που λαμβάνεται υπόψη μόνο το εσωτερικό νοσοκομείακο περιβάλλον, προκύπτουν τα εξής χαρακτηριστικά: υψηλή πολυπλοκότητα, ετερογένεια και διαφορετικοί βαθμοί ευαισθησίας, που διακρίνουν τους διαφορετικούς τύπους δεδομένων. Αυτά οδηγούν στην συνύπαρξη διαφορετικού είδους δεδομένων, στην ανάγκη για ύπαρξη διαφορετικών τύπων προσπέλασης απο τους χρήστες και την δημιουργία πληθώρας βαθμών ευαισθησίας των δεδομένων.

7.3. Το νοσοκομειακό περιβάλλον.

Ένα πραγματικό περιβάλλον εφαρμογής χρησιμοποιήθηκε το Πανεπιστημιακό Νοσοκομείο Αρεταίειο. Το Αρεταίειο Αθηνών αποτελεί τμήμα του Ιατρικού Πανεπιστημίου Αθηνών και περιλαμβάνει:

- 3 Κλινικές
- 8 Εργαστήρια
- 240 Κρεβάτια
- 86 Γιατρούς
- 142 Άτομα που ανήκουν στο νοσηλευτικό προσωπικό
- 32 Άτομα που ανήκουν στο οικονομικό τμήμα και στην γενική υποστήριξη
- 4780 Ασθενείς που νοσηλεύτηκαν το έτος 2002
- 1258 Χειρουργικές επεμβάσεις το έτος 2002 και 1209 τοκετοί
- 31.500 Εξωτερικούς ασθενείς το έτος 2002
- 687.000 Εργαστηριακές εξετάσεις το έτος 2002

Το ενιαίο πληροφοριακό σύστημα που λειτουργεί στο Αρεταίειο περιλαμβάνει εφαρμογές διαχείρησης εσωτερικών και εξωτερικών ασθενών, καθώς και εφαρμογές διοικητικής, οικονομικής και τεχνικής υποστήριξης.Το σύστημα λειτουργεί απο το 1995 και αποτελείται απο διασυνδεμένα τοπικά δίκτυα, κατανεμημένες βάσεις δεδομένων και εφαρμογές οι οποίες λειτουργούν σύνφωνα με το μοντέλο πελάτη-εξυπηρετητή. Συγκεκριμένα, τα προγράμματα εφαρμογής εκτελούνται στους σταθμούς εργασίας ή σε κατάλληλους εξυπηρετητές (servers) εφαρμογών, στους οποίους οι χρήστες έχουν πρόσβαση μέσω "κουτών" τερματικών (προσωπικών υπολογιστών με χρήση προγράμματος προσομοίωσης τερματικού). Όσο για την τοποθεσία των αποθηκευμένων δεδομένων (δύο εξυπηρετητές βάσεων δεδομένων συνδεμένοι στον "κορμό") είναι γνωστή στους τελικούς χρήστες. Επιπλέον, οι χρήστες χρησιμοποιούν τις υπηρεσίες (ηλεκτρονικό ταχυδρομεί, έρευνα κ.τ.λ.) του εκτεταμένου πανεπιστημιακού δικτύου.

7.4. Βασικά βήματα που προϋποθέτουν την ορθολογική ασφάλεια του συστήματος.

Εξαιτίας της αυξημένης δυσκολίας και πολυπλοκότητας που παρουσιάζεται για την εφαρμογή των τεχνικών διαδικασιών στην ενότητα αυτή θα περιγράψουμε πως λειτουργεί και εφαρμόζεται σ'ένα πραγματικό νοσοκομειακό περιβάλλον. Υπάρχουν δύο βήματα που αποτελούν βασικές συνιστώσες για την ασφάλεια του συστήματος.

1. Αναγνώριση των υποκειμένων και των αντικειμένων, ομαδοποιήσή τους, αναγνωρίζοντας ανάλογες λειτουργίες και ρόλους στον οργανισμό.
2. Αναγνώριση των επιτρεπτών τρόπων προσπέλασης μεταξύ των υποκειμένων και των αντικειμένων και των πιθανών συνθηκών που θα ισχύουν για αυτούς τους τρόπους προσπέλασης.

7.4.1. Αναγνώριση των υποκειμένων

Τα υποκείμενα (subjects) ενός νοσοκομείου είναι κάθε είδους άτομα, τα οποία έχουν άμεσα ή έμμεσα προσπέλαση στην βάση δεδομένων του. Γενικά, ένα υποκείμενο μπορεί να είναι ένα οποιδήποτε πρόσωπο. Για παράδειγμα, κάθε πολίτης μπορεί να τηλεφωνήσει στο νοσοκομείο για να ρωτήσει, εάν ένας ασθενής που νοσηλεύεται εκεί, έχοντας έτσι έμμεσα προσπέλαση στην νοσοκομειακή βάση δεδομένων.

Συνεπώς, τα αντικείμενα ομαδοποιούνται σε ρόλους χρήστη, ώστε να γίνει ευκολότερα η διαχείρηση της ασφάλειας στην εφαρμογή. Έτσι, ο 'τύπος' άτομο μπορεί να αναλυθεί στους εξής: ασθενής, ιατρική-υποστήριξη, προσωπικό κοστολόγισης, διαχειριστής και άλλοι τύποι ατόμου, που επιδρούν με κάποιο τρόπο, άμεσα ή έμμεσα στον ασθενή. Για παράδειγμα, η ιατρική υποστήριξη έχει πολλούς υποτύπους. Κάθε υποτύπος της ιατρικής υποστήριξης παριστάνει πολλούς διαφορετικούς τύπους εργασιών, όπως ιατροί, παραϊατρικό προσωπικό, νοσηλεύτριες, προμηθευτές εργαστηρίων και άλλα άτομα που παρέχουν ιατρικές υπηρεσίες.

Παρόμοιες διατάξεις υπάρχουν επίσης και στα υπόλοιπα τμήματα της ιεραρχίας. Έπειτα, κάθε τύπος εργασίας μπορεί να αναλυθεί σε διάφορα επίπεδα. Έτσι, ο "τύπος" Νοσηλεύτρια μπορεί να αναλυθεί στην προϊστάμενη Νοσηλεύτρια την ειδική Νοσηλεύτρια και την συνηθισμένη Νοσηλεύτρια. Ο 'τύπος' ιατρός μπορεί να αναλυθεί σε διαφορετικές ειδικότητες,όπως επικεφαλής ιατρός, εργαστηριακός ιατρός, ειδικευμένος ιατρός, κ.ο.κ. Τέλος, ο "τύπος" εργαστηριακοί θεράποντες ιατροίμπορεί να αναλυθεί στα εξής: παραϊατρικό προσωπικό, εργαστηριακούς ιατρούς, κ.τ.λ.

Στη συνέχεια θα δώσουμε τους ορισμούς των σημαντικότερων ρόλων χρήστη, δίνοντας ιδαίτερη έμφαση στις ευθύνες τους στην εφαρμογή.

- Επικεφαλής ιατρός: Είναι υπεύθυνος για την λειτουργία ενός νοσηλευτικού τμήματος (κλινικής). Δεν εμπλέκεται έμμεσα με την καθημερινή ιατρική πράξη,αλλά επιβλέπει και εποπτεύει τις δραστηριότητες όλων των θεραπόντων ιατρών του συγκεκριμένου τμήματος.
- Θεράποντας ιατρός: Αυτός εξασκεί την συνηθισμένη ιατρική πράξη (διαγνώσεις, άδειες απόλυσης, καθορισμό θεραπειών) τις εργάσιμες ώρες και σε αυτόν "χρεώνονται" συγκεκριμένοι ασθενείς.
- Εφημερεύντες ιατροί: Εξασκούν την ιατρική φροντίδα σε μη εργάσιμες μέρες και ώρες. Σε αυτούς μεταβιβάζεται η υπευθυνότητα των θεραπόντων ιατρών για το σύνολοή μέρος των ασθενώνενός τμήματος στο χρονικό διάστημα αυτό.
- Προϊστάμενη νοσηλεύτρια: Έχει διαχειριστικά και διοικητικά καθήκοντα. Αυτά περιλαμβάνουν την έκδοση των παραγγελιών των σχετικών με την νοσηλευτική φροντίδα σύμφωνα με τις οδηγίες των ιατρών και τους διαχειριστικούς κανόνες του οργανισμού, π.χ. παραγγελία εργαστηριακών εξετάσεων, έκδοση συνταγολογίων φαρμάκων, λίστες αναμονής χειρουρ-γείων, παραγγελίες υλικών, προγραμματισμός προσωπικού, κ.α.
- Νοσηλεύτριες: Αυτές είναι υπεύθυνες για την παροχή της καθημερινής νοσηλευτικής φροντίδας στους ασθενείς. Η νοσηλεύτρια μπορεί να εκτελέσει τα καθήκοντα της, χωρίς να γνωρίζει την ταυτότητα του ασθενή. Για τις

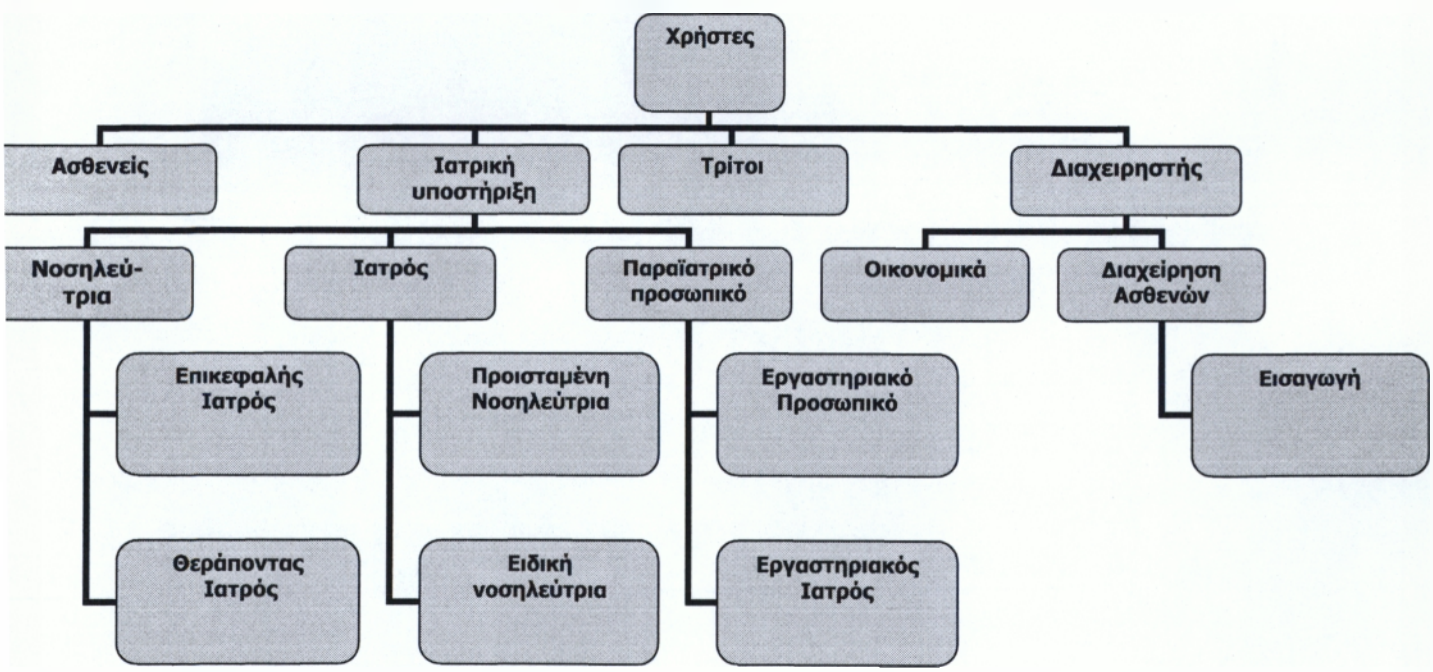
διαδικασίες αναγνώρισης χρησιμοποιείται ο (μοναδικός) αριθμός μητρώου του ασθενή σε συνδιασμό με την τοποθεσία του ασθενή (κρεβάτι, θάλαμος, χειρουργείο). Επίσης, για λόγους ασφάλειας, διακρίνουμε δύο τύπους Νοσηλευτριών:

1. τις ειδικές νοσηλεύτριες και τις
2. συνηθισμένες νοσηλεύτριες

Οι δύο τύποι διαφέρουν στο ότι μια ειδική νοσηλεύτρια θεωρείται αξιόπιστη να έχει προσπέλαση στην διάγνωση κάποιων ξεχωριστών ατόμων (V.I.P., άτομα με ευαίσθητες ασθένειες, κ.τ.λ.) ενώ δεν ισχύει το ίδιο για μία συνηθισμένη νοσηλεύτρια.

- Παραϊατρικό προσωπικό: Το προσωπικό αυτόσυλλέγει τα δείγματα (αίμα, κ.τ.λ.) και εκτελεί τις εργαστηριακές εξετάσεις (συμπεριλαμβανόμενων και των ακτινοδιαγνωστικών), που έχουν καθοριστεί για τους ασθενείς.
- Εργαστηριακοί ιατροί: Το προσωπικό αυτό επιβλέπει την εκτέλεση των εργαστηριακών εξετάσεων και κάνει την αντίστοιχη γνωμάτευση. Η συνεργασία με τον θεράποντα ιατρό για την τελική έκδοση της διάγνωσης είναι άμμεση, ιδιαίτερα σε πολύπλοκες εξετάσεις (αξονικές, μαγνητικές τομογραφίες).
- Προσωπικό οικονομικής διαχείρισης: Είναι υπεύθυνο για την συλλογή πληροφοριών, όπως δημογραφικά στοιχεία, κοινωνικά στοιχεία και ασφαλιστική κάλυψη. Επίσης, είναι υπεύθυνο για την ενημέρωση των οικονομικών στοιχείων της νοσηλείας του ασθενή και το ποσοστό που καλύπτει η ασφάλεια του ασθενή.

Έχοντας ορίσει τους ρόλους χρήστη μπορούμε να απεικονίσουμε γραφικά την ιεραρχία ώς εξής (σχήμα.2.)



Σχ.2:Η Ιεραρχία Ρόλων Χρήστη

7.4.2. Αναγνώριση των αντικειμένων

Ως αντικείμενα, τα οποία σκοπεύουμε να προστατεύσουμε,θεωρούμε όλους τους τύπους δεδομένων, οι οποίοι πιθανώς υπάρχουν σε ένα νοσοκομειακό περιβάλλον. Τα δεδομένα σε δύο κύριες κατεγορίες: τα δεδομένα που αφορούν το προσωπικό του νοσοκομείου και τα δεδομένα που αναφέρονται στους ασθενείς.

Εστιάζοντας το ενδιαφέρον μας στα δεδομένα που έχουν σχέση με τον ασθενή και που αποτελούν τον ιατρικό λογαριασμό του ασθενή, χαρακτηρίζεται συχνά απο μεγάλη πολυπλοκότητα και ετερογένεια, όσο αφορά στη φύση και στα επίπεδαευαισθησίας (sensitivity levels) των διάφορων ομάδων δεδομένων που συμπεριλαμβάνει.

Συνεπώς, η οργάνωση των δεδομένων αυτών με ένα δομημένο τρόπο είναι απαραίτητο για την ανάπτυξη των κατάλληλων 'όψεων' (views) των χρηστών και αποτελεί ένα απαραίτητο στάδιο για την σχεδίαση και την εφαρμογή ενός ασφαλούς ιατρικού συστήματος βάσεων δεδομένων. Το ακριβές σύνολο των ομάδων δεδομένων (data group) εξαρτάται, προφανώς, από το συγκεκριμένο υπό μελέτη νοσοκομειακό σύστημα.

Σύμφωνα με τα προηγούμενα ο "τύπος" αντικειμένου αγγραφής μπορεί να αναλυθεί στους εξής τύπους: το λογαριασμό αναγνώρισης ασθενή, το λογαριασμό θεραπευτικής αγωγής ασθενή, τον λογαριασμό διαχείρισης του ασθενή και άλλους τύπους. Οι τύποι αυτοί αναλύονται στην συνέχεια σε διάφορα σύνολα δεδομένων. Έτσι, ο λογαριασμός περίθαλψης ασθενή αναλύεται στα εξής: παρατηρήσεις, ιατρικές αποφάσεις, θεραπευτικές αγωγές, εργαστηριακές εξετάσεις και αποτελέσματα, κ.α. Όμοια, ο λογα-ριασμός αναγνώρισης ασθενή μπορεί να αναλυθεί σε ένα πλήθος απο διαφο-ρετικά σύνολα δεδομένα, όπως δημογραφικά δεδομένα (προσωπικά ή μη προσωπικά), ασφαλιστικά κοινωνικά, ιατρικού ιστορικού, κ.α.

Στη συνέχεια ορίζουμε τα σημαντικότερα σύνολα δεδομένων που ανήκουν σε προσανατολισμένα προς τον ασθενή δεδομένα:

- Διαχειριστικές πληροφορίες: Περιλαμβάνουνόλα τα δεδομένα, που σχετίζονται με τις διαδικασίες εξετάσεων ασθενών στα Εξωτερικά Ιατρεία (τακτικά, επείγοντα) την είσοδο-έξοδο ασθενών απο το Νοσοκομείο και την διακίνηση τους στα τμήματα του νοσοκομείου.
- Κόστος νοσηλείας: Περιλαμβάνονται τα συγκεντρωτικά στοιχεία κοστολόγησης και λογιστικής παρακολούθησης του ασθενή.
- Μη ιατρικό ιστορικό: Περιλαμβάνει πληροφορίες σχετικά με τις συνθήκες ζωής και το περιβάλλον του ασθενή (κάπνισμα, εργασία κ.τ.λ)
- Κοινωνικές πληροφορίες: Περιλαμβάνει πληροφορίες σχετικές με τα κοινωνικά και πολιτισμικά στοιχεία του ασθενή (μόρφωση, θρησκεία, ερωτική ζωή κ.τ.λ)
- Προσωπικά δημογραφικά στοιχεία: Είναι στοιχεία, όπως ο αριθμός ταυτότητας διαβατηρίου, όνομα, επώνυμο κ.α, τα οποία αναγνωρίζουν άμεσα τον ασθενή.
- Μη προσωπικά δημογραφικά στοιχεία: Περιλαμβάνονται δημογραφικά στοιχεία όπως φύλο, ευρύτερη περιοχή κατοικίας (περιοχή, νομός) κ.α. Τα

στοιχεία αυτά δε θα πρέπει να δηλώνουν τη δυνατότητα αναγνώρισης του ασθενή άμεσα ή έμμεσα. Χρησιμεύουν συνήθως για στατιστικούς σκοπούς.

- Ασφαλιστικά στοιχεία: Περιλαμβάνουν πληροφορίες σχετικά με την ασφαλιστική κάλυψη του ασθενή.
- Διαγνωστικά στοιχεία: Περιλαμβάνονται στοιχεία, όπως τα συμπτώματα το οικογενειακό ιστορικό και τις διαγνώσεις του θεράποντα ιατρού,για τον συγκεκριμένο ασθενή.
- Παραγγελίες και Αποτελέσματα εξετάσεων: Αναφέρονται στις εξετάσεις (κλινικές, εργαστηριακές, ακτινοδιαγνωστικές) που παραγγέλει ο θεράποντας ιατρός. Περιλαμβάνουν, επίσης τα αποτελέσματα των εξετάσεων αυτών και τις συσχετιζόμενες γνωματεύσεις.
- Θεραπευτική αγωγή: Περιλαμβάνει το σύνολο των θεραπευτικών αγωγών που χορηγούνται στους ασθενείς. Μπορούμε να διακρίνουμε τις ακόλουθες υποομάδες *κλινική αγωγή, θεραπευτική αγωγή, επεμβατική-χειρουργική αγωγή, ραδιοθεραπεία, φυσιοθεραπεία, δίαιτα και ψυχιατρική υποστήριξη* (με την γενικότερη έννοια) ή οποιδήποτε ομάδα αυτών των θεραπευτικών αγωγών.
- Παρατηρήσεις: Αναφέρονται στην ιατρική θεραπευτική αγωγή, την ιατρική συμπεριφορά, διαπιστώσεις κ.τ.λ.
- Αποφάσεις: Αναφέρονται στις ιατρικές διαγνώσεις, αξιολόγηση της κατάστασης της υγείας του ασθενή, μελλοντικές προβλέψεις για αυτήν κ.τ.λ.

Τα παραπάνω σύνολα δεδομένων μπορούν να απεικονιστούν γραφικά ως εξής (σχήμα 3).

Σχ.3:Η Ιεραρχία των Συνόλων Δεδομένων

7.4.3. Αναγνώριση των καταστάσεων προσπέλασης

Όπως αναφέραμε προηγουμένως, η διαγραφή απαγορεύεται συνήθως στα συστήματα ιατρικών βάσεωνδεδομένων,για λόγους ελέγχου και καταγραφής των κινήσεων. Στην εφαρμογή μας χρησιμοποιούμε μια διαδι-κασία "λογικής" διαγραφής, αντί της "φυσικής" ενημέρωσης και διαγραφής. Η διαδικασία αυτή ενεργοποιεί ένα δείκτη τριών καταστάσεων:

1. **Νέα καταχώριση** (Inserted): Η ενέργεια θα εκτελεσθεί
2. **Ακύρωση** (Cancelled): Η ενέργεια ακυρώνεται ή τερματίζεται.
3. **Ολοκλήρωση Εκτέλεσης** (Executed): Η ενέργεια έχει ολοκληρωθεί.

Για παράδειγμα,ενώ εισάγεται μια παραγγελία εργαστηριακής εξέτασης, ο δείκτης αυτός πρέπει να δείχνει "Νέα Καταχώριση". Εάν μεταφερθεί η πράξη, τότε πρέπει να δείχνει "Ολοκλήρωση εκτέλεσης". Τέλος, εάν ένας γιατρός θελήσειν να σταματήσει τις εξετάσεις, ο δείκτης θα γίνει "Ακύρωση". Η διαδικασία αυτή ακολουθείται στο πεδίο της διάγνωσης και σε όλα τα άλλα πεδία που υπονοούν ενέργειες. Η ταυτότητα του εκινητή της δράσης (Νέα Καταχώρηση, Ακύρωση, Ολοκληρωμένη Εκτέλεση) καταγράφεται, για πιθανή έρευνα της ροής των ιατρικών πληροφοριών [έλεγχος(audit)].

7.5. Απόδοση ετικετών ασφαλείας στους ρόλους χρήστη

Έχοντας χαρακτηρίσει τα αντικείμενα και τα υποκείμενα, ακολουθεί ο χαρακτηρισμός τους όσο αφορά την ασφάλεια, η λεγόμενη *ετικέτα ασφαλείας* (security label).

Σύμφωνα με τους ρόλους και τους υπορόλους που έχουν αναφερθεί κάθε χρήστης ανήκει σε μια διεύθυνση του νοσοκομείου η οποία του ορίζει τον ρόλο του ή τον υπορόλο του, ανάλογα με την θέση του στην ιεραρχική του κλίμακα του τμήματός του.

Ο χρήστης-ρόλος (admin) μπορει να προβεί σε διαγραφή, μεταβολή, προβολή, καταχώρηση όλων των στοιχείων που αφορούν την διεύθυνση στην οποία υπάγεται.

Ο χρήστης-υπορόλος (isoft) μπορει να προβεί σε διαγραφή, μεταβολή, προβολή καταχώρηση μόνο σε στοιχεία τα οποία επεξεργάζεται εκείνη την στιγμή και αφορούν το αντικείμενο της καθημερινής του εργασίας. Για κάθε συνδυασμό υπορόλου και διαλόγου ορίζεται απο την δημιουργία του προγράμματος σε ποιό A.P.P. μπορεί να εισέλθει ο χρήστης καθώςκαι τι δικαιοδοσίες έχει σ'αυτό. Ως A.P.P. ορίζεται ο πηγαίος κώδικαςόπου γίνεται η ανάπτυξητου προγράμματος.

Με αυτόν τον τρόπο διαχωρίζοντας τους χρήστες σε isoft και admin εξασφαλίζουμε την ασφάλεια του συστήματος όσο αφορά την πρόσβαση κάθε χρήστη, εγκαθιστώντας τα κατάλληλα D.L.G.

Μερικές εφαρμογές προϋποθέτουν τον καθορισμό των "κατά διάκριση" ελέγχων προσπέλασης βάση των ρόλων χρήστη. Τα περισσότερα έχουν ενσωματωμένους κανόνες, όπως τον διαχειριστή του συστήματος,το διαχειριστή της βάσης δεδομένωνκαι τον διοικητή της ασφάλειας. Πάντως είναι πιθανό οι διάφοροι χρήστες να έχουν διαφορετικές ανάγκες και ορισμούς για

τέτοιους ρόλους. Επιπλέον, πολλές εφαρμογές απαιτούν οι αυθαίρετες απαιτήσεις του ελέγχου προσπέλασης της εργασίας του χρήστη να τυποποιούνται χρησιμοποιώντας ρόλους. Συνεπώς, είναι επιθυμητή μια γενική ικανότητα για ορισμό των ρόλων απο την εφαρμογή (application-defined roles).

Τα καθορισμένα πεδία προστασίας (Named Protection Domains, N.P.D.s) μπορούν να χρησιμοποιηθούν για να προσφέρουν την δυνατότητα καθορισμού ρόλων χρήστη (user roles). Ένα καθορισμένο πεδίο προστασίας μπορεί να οριστεί για κάθε ρόλο καθορισμένο για την εφαρμογή (application-specific role). Η N.P.D. θα περιέχειτις ισχυρές, ασθενείς, θετικές και αρνητικές εξουσιοδοτήσεις, που χρειάζονται για να οριστεί ο κάθε ρόλος. Ο σχεδιαστής της εφαρμογής θα σχεδιάσει κάθε N.P.D. έτσι, ώστε να περιέχει τις συγκεκριμένες εξουσιοδοτήσεις που απαιτούνται για το ρόλο.

Για παράδειγμα, το καθορισμένο πεδίο προστασίας Μισθός Υπαλλήλου θα μπορούσε να περιέχει μια ασθενή θετική εξουσιοδότηση για να ενεργοποιήσει την μέθοδο αύξησης του μισθού στο αντικείμενο Μισθός για τα μη διοικητικά στιγμιότυπα του Μισθού. Θα μπορούσε να περιέχει ισχυρές αρνητικές εξουσιοδοτήσεις για την μέθοδο αύξησης του Μισθού και εξέτασης του Μισθού απο τον ίδιο τον υπάλληλο. Το καθορισμένο πεδίο προστασλίας Μισθός Υπαλλήλου θα μπορούσε τότε να ανατεθεί στα ανάλογα άτομα ή στις ανάλογες ομάδες.

Έτσι, οι εξουσιοδοτήσεις που έχουν σχέση με τον μισθό ενός υπαλλήλου μπορούν να ανατεθούν και να ανακληθούν από ένα διαχειριστή ασφαλείας απευθείας, χωρίς να γνωρίζει τηνιεραρχία των αντικειμένων και των λιστών εξουσιοδότησης. Εάν το σύστημα είναι σχεδιασμένο έτσι, ώστε να είναι ένα μόνο N.P.D. ενεργό κάθε φορά για ένα χρήστη, μπορεί να είναι δυνατό να υποστηριχτεί μια πολιτική διάκρισης καθηκόντων με το μηχανισμό αυτό.

Η διεύθυνση που ανήκει κάθε μέλος του προσωπικού ορίζεται απο το μητρώο προσωπικού. Οι διευθύνσεις είναι οι εξής:

Α) ΙΑΤΡΙΚΗ ΥΠΗΡΕΣΙΑ

1. Β΄ΧΕΙΡΟΥΡΓΙΚΗ ΚΛΙΝΙΚΗ. (ΚΛΙΝΕΣ 105)

ΜΟΝΑΔΕΣ (13)

- Χειρουργείου.
- Εντατικής Θεραπείας.
- Βραχείας Νοσηλείας.
- Αγγειοχειρουργικής.
- Καρδιοχειρουργικής.
- Ενδοκρινοχειρουργικής.
- Μικροχειρουργικής.
- Μαστού.

- Ενδοσκοπήσεων.
- Ανωτέρου Πεπτικού.
- Ήπατος-Χοληφόρων-Παγκρέατος.
- Παχέος Εντέρου.
- Χειρουργείου Πειραματικού.

2. ΝΕΦΡΟΛΟΓΙΚΗ ΚΛΙΝΙΚΗ. (ΚΛΙΝΕΣ 10)

ΜΟΝΑΔΕΣ (2)

- Αίθουσα τεχνητού νεφρού.
- Ερευνητικό Εργαστήριο.

4. Β΄ ΜΑΙΕΥΤΙΚΗ-ΓΥΝΑΙΚΟΛΟΓΙΚΗ ΚΛΙΝΙΚΗ.

(ΚΛΙΝΕΣ 95)+(ΝΕΟΓΝΩΝ 30)=125

ΜΟΝΑΔΕΣ (11)

- Χειρουργείου.
- Τοκετών.
- Προγεννητικού Ελέγχου.
- Οικογενειακού Προγραμματισμού.
- Στειρότητας.
- Λαμπαροσκόπησης.
- Ενδοκρινολογικής Αναπαραγωγής.
- Κυήσεων Αυξημένου Κινδύνου.
- Εξωσωματικής Γονιμότητας.
- Εντατικής Νεογέννητων.

4. ΕΡΓΑΣΤΗΡΙΟ ΑΚΤΙΝΟΛΟΓΙΑΣ.

ΜΟΝΑΔΕΣ (10)

- Συμβατικής Ακτινοδιαγνωστικής.
- Υπερήχων.
- Αξονικής και Μαγνητικής Τομογραφίας.
- Αγγειογραφίας.
- Πυρηνικής Ιατρικής.
- Ακτινοδιαγνωστικής.
- Ιατρικής Φυσικής.
- Υπερθερμίας.
- Ιατρικής Φωτογραφίας.
- Ογκολογίας (κοινή μετά των άλλων κλινικών-εργαστηρίων).

5. ΕΡΓΑΣΤΗΡΙΑ ΚΑΙ ΕΙΔΙΚΕΣ ΜΟΝΑΔΕΣ.

- Μονάδα Αναισθησιολογίας.
- Σταθμός Αιμοδοσίας.
- Μικροβιολογικό.
- Παθολογοανατομικό.
- Κυτταρολογικό.
- Βιοχημικό.
- Ορμονολογικό.

6. ΕΞΩΤΕΡΙΚΑ ΙΑΤΡΕΙΑ.

Σε κάθε κλινική και ειδική μονάδα λειτουργούν αντίστοιχα τακτικά Εξωτερικά Ιατρεία.

7. ΦΑΡΜΑΚΕΥΤΙΚΟ ΤΜΗΜΑ.

Β΄ ΝΟΣΗΛΕΥΤΙΚΗ ΥΠΗΡΕΣΙΑ.

Η Νοσηλευτική Υπηρεσία διαρθρώνεται σε τρεις (3) τομείς.

Α) 1ος τομέας σε (8) Νοσηλευτικά Τμήματα που καλύπτουν τις ανάγκες των χειρουργικών και της Νεφρολογικής Κλινικής.

Β) 2ος τομέας σε (8) Νοσηλευτικά Τμήματα που καλύπτουν τις ανάγκες της Μαιευτικής-Γυναικολογικής Κλίνικής.

Γ) 3ος τομέας σε (8) Νοσηλευτικά Τμήματα που καλύπτουν τις ανάγκες των Εργαστηρίων και τν Εξωτερικών Ιατρείων.

Γ΄ ΔΙΟΙΚΗΤΙΚΗ ΥΠΗΡΕΣΙΑ:

ΔΙΕΥΘΥΝΣΕΙΣ:

Α. Διεύθυνση Διοικητικού.
Β. Διεύθυνση Οικονομικού.
Γ. Διεύθυνση Τεχνικού.

ΔΙΑΡΘΡΩΣΗ ΣΕ ΤΜΗΜΑΤΑ ΚΑΙ ΑΥΤΟΤΕΛΗ ΓΡΑΦΕΙΑ:

Α) Διεύθυνση Διοικητικού

- Τμήμα Προσωπικού.
- Τμήμα Γραμματείας.
- Τμήμα Παρακολούθησης Ασθενών και Αρχείου.
- Τμήμα Επιστασίας.
- Γραφείο Βιβλιοθήκης.

Β) Διεύθυνση Οικονομικού

- Τμήμα Λογιστηρίου.
- Τμήμα Προμηθειών.
- Τμήμα Διαχείρησης.
- Τμήμα Χρηματικού.
- Τμήμα Πληροφορικής και Οργάνωσης.
- Τμήμα Διατροφής.

Γ) Διεύθυνση Τεχνικού.

- Τμήμα Τεχνικών Έργων.
- Τμήμα Βιοϊατρικής Τεχνολογίας.

ΠΑΡΑΡΤΗΜΑ

Ο ΔΙΕΥΘΥΝΤΗΣ

ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ
ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΤΕΥΧΟΣ ΠΡΩΤΟ Αρ. Φύλλου 50

10 Απριλίου 1997

ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 2472

Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Ο ΠΡΟΕΔΡΟΣ
ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

Εκδίδομε τον ακόλουθο νόμο που ψήφισε η Βουλή:

ΚΕΦΑΛΑΙΟ Α'
ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1
Αντικείμενο

Αντικείμενο του παρόντος νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής.

Άρθρο 2
Ορισμοί

Για τους σκοπούς του παρόντος νόμου νοούνται ως:

α) "Δεδομένα προσωπικού χαρακτήρα", κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

β) "Ευαίσθητα δεδομένα", τα δεδομένα που αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, την υγεία, την κοινωνική πρόνοια και την ερωτική ζωή, καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες.

γ) "Υποκείμενο των δεδομένων", το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

δ) "Επεξεργασία δεδομένων προσωπικού χαρακτήρα" ("επεξεργασία"), κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή.

ε) "Αρχείο δεδομένων προσωπικού χαρακτήρα" ("αρχείο"), σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία αποτελούν ή μπορεί να αποτελέσουν αντικείμενο επεξεργασίας, και τα οποία τηρούνται είτε από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο.

στ) "Διασύνδεση", μορφή επεξεργασίας που συνίσταται στη δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από άλλον ή άλλους υπεύθυνους επεξεργασίας ή που τηρούνται από τον ίδιο υπεύθυνο επεξεργασίας για άλλο σκοπό.

ζ) "Υπεύθυνος επεξεργασίας", οποιοσδήποτε καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο.

η) "Εκτελών την επεξεργασία", οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή

νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

θ) "Τρίτος", κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας και τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, εφόσον ενεργούν υπό την άμεση εποπτεία ή για λογαριασμό του υπεύθυνου επεξεργασίας.

ι) "Αποδέκτης", το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως αν πρόκειται για τρίτο ή όχι.

ια) "Συγκατάθεση" του υποκειμένου των δεδομένων, κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή και εν πλήρη επιγνώσει και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελούν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για το σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.

ιβ) "Αρχή", η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που θεσπίζεται στο κεφάλαιο Δ' του παρόντος νόμου.

Άρθρο 3
Πεδίο εφαρμογής

1. Οι διατάξεις του παρόντος νόμου εφαρμόζονται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία, καθώς και στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο.

2. Οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία πραγματοποιείται από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών.

3. Ο παρών νόμος εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον αυτή εκτελείται:

α) Από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο, όπου βάσει του δημοσίου διεθνούς δικαίου, εφαρμόζεται το ελληνικό δίκαιο.

β) Από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο, όπου εφαρμόζεται το ελληνικό δίκαιο, όταν η επεξεργασία αφορά υποκείμενα εγκατεστημένα στην Ελληνική Επικράτεια. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την Αρχή εκπρόσωπο εγκατεστημένο στην Ελληνική Επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και υποχρεώσεις του υπευθύνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του. Το αυτό ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από διπλωματικά, consular ή άλλο λόγο που κωλύει την ποινική δίωξη.

γ) Από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος στην επικράτεια Κράτους-Μέλους της Ευρωπαϊκής Ένωσης αλλά τρίτης χώρας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στην Ελληνική Επικράτεια, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από αυτήν. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την Αρχή εκπρόσωπο εγκατεστημένο στην Ελληνική Επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και υποχρεώσεις του υπευθύνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του. Το αυτό ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από διπλωματικά, consular ή άλλο λόγο που κωλύει την ποινική δίωξη.

ΚΕΦΑΛΑΙΟ Β'
ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Άρθρο 4
Χαρακτηριστικά δεδομένων προσωπικού χαρακτήρα

1. Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει:

α) Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία εν όψει των σκοπών αυτών.

β) Να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.

γ) Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.

δ) Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Μετά την περάτωση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς, επιστημονικούς ή στατιστικούς σκοπούς, εφόσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων. Η τήρηση των διατάξεων της παραγράφου αυτής βαρύνει τον υπεύθυνο επεξεργασίας.

2. Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεγεί ή υφίστανται επεξεργασία, κατά παράβαση της προηγούμενης παραγράφου, καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας. Η Αρχή, εάν εξακριβώσει αυτεπαγγέλτως ή μετά από σχετική καταγγελία παράβαση των διατάξεων της προηγούμενης παραγράφου, επιβάλλει τη διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των δεδομένων προσωπικού χαρακτήρα που έχουν ήδη συλλεγεί ή τύχει επεξεργασίας.

Άρθρο 5
Προϋποθέσεις επεξεργασίας

1. Επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του.

2. Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, όταν:

α) Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο.

β) Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.

γ) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

δ) Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα.

ε) Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.

3. Η Αρχή μπορεί να εκδίδει ειδικούς κανόνες επεξεργασίας για τις πλέον συνήθεις κατηγορίες επεξεργασιών και αρχείων, οι οποίες προφανώς δεν θίγουν τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα. Οι κατηγορίες αυτές προσδιορίζονται με κανονισμούς που καταρτίζει η Αρχή και κυρώνονται με προεδρικά διατάγματα, τα οποία εκδίδονται με πρόταση του Υπουργού Δικαιοσύνης.

Άρθρο 6
Γνωστοποίηση

1. Ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας.

2. Με τη γνωστοποίηση της προηγούμενης παραγράφου ο υπεύθυνος επεξεργασίας πρέπει απαραιτήτως να δηλώνει:

α) Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο του, καθώς και τη διεύθυνση του, καθώς και το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο και τη διεύθυνση των προσώπων που χρησιμοποιεί για την εκτέλεση της επεξεργασίας σύμφωνα με το άρθρο 10. Εάν ο υπεύθυνος επεξεργασίας δεν είναι εγκατεστημένος στην Ελληνική Επικράτεια ή σε τόπο, όπου εφαρμόζεται το ελληνικό δίκαιο, θα πρέπει επιπροσθέτως να δηλώνεται το ονοματεπώνυμο ή η επωνυμία ή ο τίτλος και η διεύθυνση του εκπροσώπου του στην Ελλάδα.

β) Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο ή ο κύριος εξοπλισμός που υποστηρίζει την επεξεργασία.

γ) Την περιγραφή του σκοπού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.

δ) Το είδος των δεδομένων προσωπικού χαρακτήρα που υφίστανται ή πρόκειται να υποστούν επεξεργασία ή περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.

ε) Το χρονικό διάστημα για το οποίο προτίθεται να εκτελεί την επεξεργασία ή να διατηρήσει το αρχείο.

στ) Τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους ανακοινώνει ή ενδέχεται να ανακοινώνει τα δεδομένα προσωπικού χαρακτήρα.

ζ) Τις ενδεχόμενες διαβιβάσεις και το σκοπό της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες.

η) Τα βασικά χαρακτηριστικά του συστήματος και των μέτρων ασφαλείας του αρχείου ή της επεξεργασίας.

θ) Στην περίπτωση που η επεξεργασία ή το αρχείο εμπίπτει σε μία από τις κατηγορίες για τις οποίες η Αρχή έχει εκδώσει ειδικούς κανόνες επεξεργασίας, ο υπεύθυνος επεξεργασίας καταθέτει στην Αρχή δήλωση με την οποία βεβαιώνει ότι η επεξεργασία θα διεξάγεται ή το αρχείο θα τηρείται σύμφωνα με τους ειδικούς κανόνες που έχει θεσπίσει η Αρχή, η οποία προσδιορίζει ειδικότερα τον τύπο και το περιεχόμενο της δήλωσης.

3. Τα στοιχεία της προηγούμενης παραγράφου καταχωρίζονται στο Μητρώο Αρχείων και Επεξεργασιών που τηρεί η Αρχή.

4. Κάθε μεταβολή των στοιχείων που αναφέρονται στην παράγραφο 2 πρέπει να γνωστοποιείται εγγράφως και χωρίς καθυστέρηση από τον υπεύθυνο στην Αρχή.

Άρθρο 7
Επεξεργασία ευαίσθητων δεδομένων

1. Απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων.

2. Κατ' εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής, όταν συντρέχουν μία ή περισσότερες από τις ακόλουθες προϋποθέσεις:

α) Το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή τα χρηστά ήθη ή νόμος ορίζει ότι η συγκατάθεση δεν αίρει την απαγόρευση.

β) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν τούτο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

γ) Η επεξεργασία αφορά αποκλειστικά δεδομένα που το υποκείμενο, τα οποία δημοσιοποιεί ή που είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματός του ενώπιον δικαστηρίου.

δ) Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.

ε) Η επεξεργασία είναι απαραίτητη για την εξυπηρέτηση των αναγκών της εθνικής ασφάλειας, καθώς επίσης και για την εξυπηρέτηση των αναγκών της εγκληματολογικής ή σωφρονιστικής πολιτικής, όταν εκτελείται από δημόσια Αρχή και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες και μέτρα ασφαλείας.

στ) Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.

Ζ) Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος. Η άδεια της αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για την εξασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης και εφόσον δεν παραβιάζεται καθ' οιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής.

3. Η Αρχή χορηγεί άδεια συλλογής και επεξεργασίας ευαίσθητων δεδομένων, καθώς και άδεια ιδρύσεως και λειτουργίας σχετικού αρχείου, ύστερα από αίτηση του υπεύθυνου επεξεργασίας. Εφόσον η Αρχή διαπιστώσει ότι πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων, η γνωστοποίηση αρχείου, σύμφωνα με το άρθρο 6 του παρόντος νόμου, επέχει θέση αίτησης για τη χορήγηση άδειας. Η Αρχή μπορεί να επιβάλλει όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων. Πριν χορηγήσει την άδεια, η Αρχή καλεί σε ακρόαση τον υπεύθυνο επεξεργασίας ή τον εκπρόσωπό του και τον εκτελούντα την επεξεργασία.

4. Η άδεια εκδίδεται για ορισμένο χρόνο, ανάλογα με το σκοπό της επεξεργασίας. Μπορεί να ανανεωθεί ύστερα από αίτηση του υπεύθυνου επεξεργασίας.

5. Η άδεια περιέχει απαραιτήτως:

α) Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο, καθώς και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του.

β) Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο.

γ) Το είδος των δεδομένων προσωπικού χαρακτήρα που επιτρέπεται να περιληφθούν στο αρχείο.

δ) Το χρονικό διάστημα για το οποίο χορηγείται η άδεια.

ε) Τους τυχόν όρους και προϋποθέσεις που έχει επιβάλει η Αρχή για την ίδρυση και λειτουργία του αρχείου.

στ) Την υποχρέωση γνωστοποίησης του ή των αποδεκτών ευθύς ως εξατομικευθούν.

6. Αντίγραφο της άδειας καταχωρίζεται στο Μητρώο αρχείων που διατηρεί η Αρχή.

7. Κάθε μεταβολή των στοιχείων που αναφέρονται στην παράγραφο 5 γνωστοποιείται χωρίς καθυστέρηση στην Αρχή. Κάθε άλλη μεταβολή, πλην της διεύθυνσης του υπεύθυνου ή του εκπροσώπου του, συνεπάγεται έκδοση νέας άδειας, εφόσον συντρέχουν οι νόμιμες προϋποθέσεις.

Άρθρο 8
Διασύνδεση αρχείων

1. Διασύνδεση αρχείων επιτρέπεται μόνον υπό τους όρους του παρόντος άρθρου.

2. Κάθε διασύνδεση γνωστοποιείται στην Αρχή με δήλωση την οποία υποβάλλουν από κοινού οι υπεύθυνοι επεξεργασίας ή ο υπεύθυνος επεξεργασίας, που διασυνδέει δύο ή περισσότερα αρχεία που εξυπηρετούν διαφορετικούς σκοπούς.

3. Εάν ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα ή εάν η διασύνδεση έχει ως συνέπεια την αποκάλυψη ευαίσθητων δεδομένων ή εάν για την πραγματοποίηση της διασύνδεσης πρόκειται να γίνει χρήση ενιαίου κωδικού αριθμού, η διασύνδεση επιτρέπεται μόνο με προηγούμενη άδεια της Αρχής (άδεια διασύνδεσης).

4. Η άδεια διασύνδεσης της προηγούμενης παραγράφου χορηγείται ύστερα από ακρόαση των υπεύθυνων επεξεργασίας των αρχείων και περιέχει απαραιτήτως:

α) Το σκοπό για τον οποίο η διασύνδεση θεωρείται αναγκαία.

β) Το είδος των δεδομένων προσωπικού χαρακτήρα που αφορά η διασύνδεση.

γ) Το χρονικό διάστημα για το οποίο επιτρέπεται η διασύνδεση.

δ) Τους τυχόν όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία των δικαιωμάτων και ελευθεριών και ιδίως του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων.

5. Η άδεια διασύνδεσης μπορεί να ανανεωθεί ύστερα από αίτηση των υπεύθυνων επεξεργασίας.

6. Οι δηλώσεις της παρ. 2 του παρόντος άρθρου, καθώς και αντίγραφα των αδειών διασύνδεσης καταχωρίζονται στο Μητρώο Διασυνδέσεων που τηρεί η Αρχή.

Άρθρο 9
Διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα

1. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε χώρες της Ευρωπαϊκής Ένωσης είναι ελεύθερη. Η διαβίβαση προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση δεδομένων προσωπικού χαρακτήρα, τα οποία έχουν υποστεί ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται ύστερα από άδεια της Αρχής. Η Αρχή παρέχει την άδεια μόνον εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Προς τούτο, λαμβάνει υπόψη ιδίως τη φύση των δεδομένων, τους σκοπούς και τη διάρκεια της επεξεργασίας, τους σχετικούς γενικούς και ειδικούς κανόνες δικαίου, τους κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων.

2. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση και η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ' εξαίρεση, με άδεια της

Αρχής, εφόσον συντρέχει μία ή περισσότερες από τις κατωτέρω προυποθέσεις:

α) Το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του για τη διαβίβαση, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που να αντίκειται στο νόμο ή τα χρηστά ήθη.

β) Η διαβίβαση είναι απαραίτητη: i) για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων, εφόσον αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, ή ii) για τη συνομολόγηση και εκτέλεση σύμβασης μεταξύ αυτού και του υπευθύνου επεξεργασίας ή μεταξύ του υπευθύνου επεξεργασίας και τρίτου προς το συμφέρον του υποκειμένου των δεδομένων, εφόσον το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, ή iii) για την εκτέλεση προσυμβατικών μέτρων που έχουν ληφθεί κατ' αίτηση του υποκειμένου των δεδομένων.

γ) Η διαβίβαση είναι απαραίτητη για την αντιμετώπιση εξαιρετικής ανάγκης και τη διαφύλαξη υπέρτερου δημοσίου συμφέροντος, ιδίως για την εκτέλεση συμβάσεων συνεργασίας με δημόσιες Αρχές της άλλης χώρας, εφόσον ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και την άσκηση των σχετικών δικαιωμάτων.

δ) Η διαβίβαση είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον του δικαστηρίου.

ε) Η μετάδοση πραγματοποιείται από δημόσιο μητρώο, το οποίο κατά το νόμο προορίζεται για την παροχή πληροφοριών στο κοινό και είναι προσιτό στο κοινό ή σε κάθε πρόσωπο που αποδεικνύει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι νόμιμες προυποθέσεις για την πρόσβαση στο μητρώο.

3. Στις περιπτώσεις των προηγούμενων παραγράφων η Αρχή ενημερώνει την Ευρωπαική Επιτροπή και τις αντίστοιχες Αρχές των άλλων Κρατών-Μελών, όταν θεωρεί ότι μία χώρα δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας.

Άρθρο 10
Απόρρητο και ασφάλεια της επεξεργασίας

1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απορρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνο κατ' εντολήν του.

2. Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

3. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Η Αρχή παρέχει εκάστοτε οδηγίες για το βαθμό ασφάλειας των δεδομένων, καθώς και για τα μέτρα προστασίας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία δεδομένων, εν όψει και των τεχνολογικών εξελίξεων.

4. Αν η επεξεργασία διεξάγεται για λογαριασμό του υπευθύνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει υποχρεωτικά ότι ο ενεργών την επεξεργασία τη διεξάγει μόνο κατ' εντολήν του υπευθύνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν.

ΚΕΦΑΛΑΙΟ Γ'
ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Άρθρο 11
Δικαίωμα ενημέρωσης

1. Ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία:

α) την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του,

β) το σκοπό της επεξεργασίας,

γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων,

δ) την ύπαρξη του δικαιώματος πρόσβασης.

2. Εάν για τη συλλογή των δεδομένων προσωπικού χαρακτήρα ο υπεύθυνος επεξεργασίας ζητά τη συνδρομή του υποκειμένου, οφείλει να το ενημερώνει ειδικώς και εγγράφως για τα στοιχεία της παρ. 1 του παρόντος άρθρου, καθώς και για τα δικαιώματά του, σύμφωνα με τα άρθρα 11 έως και 13 του παρόντος νόμου. Με την αυτή ενημέρωση ο υπεύθυνος επεξεργασίας γνωστοποιεί στο υποκείμενο εάν υποχρεούται ή όχι να παράσχει τη συνδρομή του, με βάση ποιες διατάξεις, καθώς και για τις τυχόν συνέπειες της αρνήσεώς του.

3. Εάν τα δεδομένα ανακοινώνονται σε τρίτους, το υποκείμενο ενημερώνεται για την ανακοίνωση πριν από αυτούς.

4. Με απόφαση της Αρχής, ύστερα από αίτηση του υπευθύνου επεξεργασίας, η υποχρέωση ενημέρωσης, σύμφωνα με τις παρ. 1 και 3 του παρόντος άρθρου, μπορεί να αρθεί, εν όλω ή εν μέρει, εφόσον η συλλογή δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφαλείας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

5. Με την επιφύλαξη των δικαιωμάτων εκ των άρθρων 12 και 13, η υποχρέωση ενημέρωσης δεν υφίσταται όταν η συλλογή γίνεται αποκλειστικά για δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα.

Άρθρο 12
Δικαίωμα πρόσβασης

1. Καθένας έχει δικαίωμα να γνωρίζει εάν δεδομένα προσωπικού χαρακτήρα που τον αφορούν αποτελούν

ή αποτελούσαν αντικείμενο επεξεργασίας. Προς τούτο, ο υπεύθυνος επεξεργασίας έχει υποχρέωση να του απαντήσει εγγράφως.

2. Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή, τις ακόλουθες πληροφορίες:

α) Όλα τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν, καθώς και την προέλευσή τους.

β) Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών.

γ) Την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση ή πληροφόρησή του.

δ) Τη λογική της αυτοματοποιημένης επεξεργασίας.

Το δικαίωμα πρόσβασης μπορεί να ασκείται από το υποκείμενο των δεδομένων και με τη συνδρομή αδειού.

3. Το δικαίωμα της προηγούμενης παραγράφου και τα δικαιώματα του άρθρου 13 ασκούνται με την υποβολή της σχετικής αίτησης στον υπεύθυνο της επεξεργασίας και ταυτόχρονη καταβολή χρηματικού ποσού, το ύψος του οποίου, ο τρόπος καταβολής του και κάθε άλλο συναφές ζήτημα ρυθμίζονται με απόφαση της Αρχής. Το ποσό αυτό επιστρέφεται στον αιτούντα εάν το αίτημα διόρθωσης ή διαγραφής των δεδομένων κριθεί βάσιμο είτε από τον υπεύθυνο της επεξεργασίας είτε από την Αρχή, σε περίπτωση προσφυγής του σε αυτήν. Ο υπεύθυνος έχει υποχρέωση στην περίπτωση αυτή να χορηγήσει στον αιτούντα, χωρίς καθυστέρηση δωρεάν και σε γλώσσα κατανοητή, αντίγραφο του διορθωμένου μέρους της επεξεργασίας που τον αφορά.

4. Εάν ο υπεύθυνος επεξεργασίας δεν απαντήσει εντός δεκαπέντε (15) ημερών ή εάν η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει δικαίωμα να προσφύγει στην Αρχή. Στην περίπτωση κατά την οποία ο υπεύθυνος επεξεργασίας αρνηθεί να ικανοποιήσει το αίτημα του ενδιαφερομένου, κοινοποιεί την απάντησή του στην Αρχή και ενημερώνει τον ενδιαφερόμενο ότι μπορεί να προσφύγει σε αυτήν.

5. Με απόφαση της Αρχής, ύστερα από αίτηση του υπεύθυνου επεξεργασίας, η υποχρέωση πληροφόρησης, σύμφωνα με τις παρ. 1 και 2 του παρόντος άρθρου, μπορεί να αρθεί εν όλω ή εν μέρει, εφόσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στην περίπτωση αυτή ο Πρόεδρος της Αρχής ή ο αναπληρωτής του προβαίνει σε όλες τις αναγκαίες ενέργειες και έχει ελεύθερη πρόσβαση στο αρχείο.

6. Δεδομένα που αφορούν την υγεία γνωστοποιούνται στο υποκείμενο μέσω ιατρού.

Άρθρο 13
Δικαίωμα αντίρρησης

1. Το υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία δεδομένων που το αφορούν. Οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχουν αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών. Στην απάντησή του οφείλει να ενημερώσει το υποκείμενο για τις ενέργειες στις οποίες προέβη ή, ενδεχομένως, για τους λόγους που δεν ικανοποίησε το αίτημα. Η απάντηση σε περίπτωση απόρριψης των αντιρρήσεων πρέπει να κοινοποιείται και στην Αρχή.

2. Εάν ο υπεύθυνος επεξεργασίας δεν απαντήσει εμπροθέσμως ή η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει δικαίωμα να προσφύγει στην Αρχή και να ζητήσει την εξέταση των αντιρρήσεών του. Εάν η Αρχή πιθανολογήσει ότι οι αντιρρήσεις είναι εύλογες και ότι συντρέχει κίνδυνος σοβαρής βλάβης του υποκειμένου από τη συνέχιση της επεξεργασίας, μπορεί να επιβάλλει την άμεση αναστολή της επεξεργασίας έως ότου εκδώσει οριστική απόφαση επί των αντιρρήσεων.

3. Καθένας έχει δικαίωμα να δηλώσει στην Αρχή ότι δεδομένα που τον αφορούν δεν επιθυμεί να αποτελέσουν αντικείμενο επεξεργασίας από οποιονδήποτε, για λόγους προώθησης πωλήσεως αγαθών ή παροχής υπηρεσιών εξ αποστάσεως. Η Αρχή τηρεί μητρώο με τα στοιχεία ταυτότητας των ενωτέρω. Οι υπεύθυνοι επεξεργασίας των σχετικών αρχείων έχουν την υποχρέωση να συμβουλεύονται πριν από κάθε επεξεργασία το εν λόγω μητρώο και να διαγράφουν από το αρχείο τους τα πρόσωπα της παραγράφου αυτής.

Άρθρο 14
Δικαίωμα προσωρινής δικαστικής προστασίας

1. Καθένας έχει δικαίωμα να ζητήσει από το αρμόδιο κάθε φορά δικαστήριο την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, την οποία έχει λάβει διοικητική αρχή ή νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, εφόσον η επεξεργασία αυτή αποβλέπει στην αξιολόγηση της προσωπικότητός του και ιδίως της αποδοτικότητάς του στην εργασία, της οικονομικής φερεγγυότητάς του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του.

2. Το δικαίωμα του παρόντος άρθρου μπορεί να ικανοποιηθεί και όταν δεν συντρέχουν οι λοιπές ουσιαστικές προϋποθέσεις της προσωρινής δικαστικής προστασίας, όπως προβλέπονται κάθε φορά.

ΚΕΦΑΛΑΙΟ Δ'
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Άρθρο 15
Σύσταση - Αποστολή - Νομική φύση

1. Συνιστάται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Αρχή), με αποστολή την εποπτεία της εφαρμογής του παρόντος νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά.

2. Η Αρχή αποτελεί ανεξάρτητη δημόσια αρχή, έχει δικό της προυπολογισμό και εξυπηρετείται από δική της γραμματεία. Η Αρχή δεν υπόκειται σε οποιονδήποτε διοικητικό έλεγχο. Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής απολαύουν προσωπικής και λειτουργικής ανεξαρτησίας. Η Αρχή υπάγεται στον Υπουργό Δικαιοσύνης και εδρεύει στην Αθήνα.

3. Τον προυπολογισμό της Αρχής εισηγείται ο Υπουργός Δικαιοσύνης, ύστερα από πρόταση της Αρχής. Ποσοστό των κάθε είδους εσόδων του Δημοσίου από την εφαρμογή του παρόντος νόμου, συμπεριλαμβανομένων των παραβόλων και προστίμων που επιβάλλει η Αρχή, διατίθεται για τις ανάγκες της Αρχής. Το ποσοστό αυτό καθορίζεται κάθε φορά με κοινή απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης.

Άρθρο 16
Συγκρότηση της Αρχής

1. Η Αρχή συγκροτείται από ένα δικαστικό λειτουργό βαθμού Συμβούλου της Επικρατείας ή αντίστοιχου και άνω, ως Πρόεδρο, και έξι μέλη ως εξής:

α) Έναν καθηγητή ή αναπληρωτή καθηγητή Α.Ε.Ι. σε γνωστικό αντικείμενο του δικαίου.

β) Έναν καθηγητή ή αναπληρωτή καθηγητή Α.Ε.Ι. σε γνωστικό αντικείμενο της πληροφορικής.

γ) Έναν καθηγητή ή αναπληρωτή καθηγητή Α.Ε.Ι.

δ, ε, στ) Τρία πρόσωπα κύρους και εμπειρίας στον τομέα της προστασίας δεδομένων προσωπικού χαρακτήρα.

Ο δικαστικός λειτουργός - Πρόεδρος και οι καθηγητές-μέλη μπορεί να είναι εν ενεργεία ή μη.

2. Ο Πρόεδρος της Αρχής είναι πλήρους και αποκλειστικής απασχόλησης και διορίζεται με προεδρικό διάταγμα, που εκδίδεται με πρόταση του Υπουργικού Συμβουλίου, ύστερα από εισήγηση του Υπουργού Δικαιοσύνης. Εάν για τη θέση του Προέδρου επιλεγεί εν ενεργεία δικαστικός λειτουργός, απαιτείται απόφαση του οικείου Ανώτατου Δικαστικού Συμβουλίου. Με την ίδια διαδικασία επιλέγεται και διορίζεται ο αναπληρωτής του Προέδρου.

3. Τα μέλη της Αρχής διορίζονται με την εξής διαδικασία: ο Υπουργός Δικαιοσύνης υποβάλλει στον Πρόεδρο της Βουλής πρόταση για το διορισμό των έξι τακτικών μελών της Αρχής και των ισαρίθμων αναπληρωτών τους. Η πρόταση περιλαμβάνει διπλάσιο αριθμό υποψηφίων. Ο Πρόεδρος της Βουλής διαβιβάζει την πρόταση στην Επιτροπή Θεσμών και Διαφάνειας, η οποία διατυπώνει γνώμη. Τα τακτικά μέλη της Αρχής και οι αντίστοιχοι αναπληρωτές τους επιλέγονται από τη Διάσκεψη των Προέδρων. Οι επιλεγέντες διορίζονται με προεδρικό διάταγμα, που εκδίδεται με πρόταση του Υπουργού Δικαιοσύνης και δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως.

4. Ο Πρόεδρος και τα μέλη της Αρχής διορίζονται με θητεία. Η θητεία τους είναι τετραετής και μπορεί να ανανεωθεί μία μόνο φορά. Κανείς δεν μπορεί να υπηρετήσει συνολικά περισσότερο από οκτώ (8) χρόνια. Η σύνθεση των έξι μελών της Αρχής ανανεώνεται κατά το ήμισυ ανά διετία. Μετά την πρώτη συγκρότηση της Αρχής, γίνεται κλήρωση μεταξύ των έξι τακτικών μελών της, ώστε τρία να έχουν τετραετή θητεία και τρία διετή.

5. Ο Πρόεδρος και τα μέλη της Αρχής διορίζονται με ισάριθμους αναπληρωτές, οι οποίοι πρέπει να διαθέτουν τις αυτές ιδιότητες και προσόντα. Οι αναπληρωτές του Προέδρου και των μελών μετέχουν στις συνεδριάσεις της Αρχής μόνο σε περίπτωση προσωρινής απουσίας ή κωλύματος του αντίστοιχου τακτικού. Με απόφασή του ο Πρόεδρος της Αρχής αναθέτει ειδικά καθήκοντα στους αναπληρωτές. Η θητεία του κάθε αναπληρωτή είναι ίση με τη θητεία του αντίστοιχου τακτικού.

Άρθρο 17
Κωλύματα - Ασυμβίβαστα μελών της Αρχής

1. Δεν μπορεί να διορισθεί μέλος της Αρχής:

α) Υπουργός, υφυπουργός, γενικός γραμματέας υπουργείου ή αυτοτελούς γενικής γραμματείας και βουλευτής.

β) Διοικητής, διευθυντής, διαχειριστής, μέλος του διοικητικού συμβουλίου ή άσκων διευθυντικά καθήκοντα εν γένει σε επιχείρηση η οποία παράγει, μεταποιεί, διαθέτει ή εμπορεύεται υλικά χρησιμοποιούμενα στην πληροφορική ή τις τηλεπικοινωνίες ή παρέχει υπηρεσίες σχετικές με την πληροφορική, τις τηλεπικοινωνίες ή την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και οι συνδεόμενοι με σύμβαση έργου με τέτοια επιχείρηση.

2. Εκπίπτει αυτοδικαίως από την ιδιότητα του μέλους της Αρχής όποιος, μετά το διορισμό του:

α) Αποκτά μία από τις ιδιότητες που συνιστούν κώλυμα διορισμού, σύμφωνα με την προηγούμενη παράγραφο.

β) Προβαίνει σε πράξεις ή αναλαμβάνει οποιαδήποτε εργασία ή έργο ή αποκτά άλλη ιδιότητα που, κατά την κρίση της Αρχής, δεν συμβιβάζονται με τα καθήκοντα του ως μέλους της Αρχής.

3. Στη διαπίστωση των ασυμβίβαστων της προηγούμενης παραγράφου προβαίνει η Αρχή, χωρίς συμμετοχή του μέλους της, στο πρόσωπο του οποίου ενδέχεται να συντρέχει το ασυμβίβαστο. Η Αρχή αποφασίζει ύστερα από ακρόαση του εν λόγω μέλους. Τη διαδικασία κινεί είτε ο Πρόεδρος της Αρχής είτε ο Υπουργός Δικαιοσύνης.

4. Απώλεια της ιδιότητος βάσει της οποίας μέλος της Αρχής διορίσθηκε, σύμφωνα με την παρ. 1 του άρθρου 15 του παρόντος νόμου, συνεπάγεται την αυτοδίκαιη έκπτωσή του, αν οφείλεται σε αμετάκλητη πειθαρχική ή ποινική καταδίκη.

Άρθρο 18
Υποχρεώσεις και δικαιώματα μελών της Αρχής

1. Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής υπακούουν στη συνείδησή τους και το νόμο. Υπόκεινται στο καθήκον εχεμύθειας. Ως μάρτυρες ή πραγματογνώμονες μπορούν να καταθέτουν στοιχεία που αφορούν αποκλειστικά και μόνο την τήρηση των διατάξεων του παρόντος νόμου από υπεύθυνους επεξεργασίας. Το καθήκον εχεμύθειας υφίσταται και μετά την με οποιονδήποτε τρόπο αποχώρηση των μελών της Αρχής.

2. Με απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης καθορίζονται οι μηνιαίες αποδοχές του Προέ-

δρου και των μελών της Αρχής, καθώς και η αποζημίωσή τους για κάθε συνεδρίαση, κατά παρέκκλιση από κάθε άλλη διάταξη. Στους αναπληρωτές καταβάλλεται το ένα τρίτο (1/3) των μηνιαίων αποδοχών των μελών της Αρχής και αποζημίωση για κάθε συνεδρίαση στην οποία μετέχουν. Οι διατάξεις για τις δαπάνες κίνησεως των μετακινούμενων προσώπων με εντολή του Δημοσίου για εκτέλεση υπηρεσίας που ισχύουν κάθε φορά έχουν εφαρμογή και για τη μετακίνηση των μελών και των υπαλλήλων της Γραμματείας της Αρχής. Ο Πρόεδρος της Αρχής εκδίδει τις σχετικές εντολές μετακίνησης.

3. Για κάθε παράβαση των υποχρεώσεών τους που απορρέουν από τον παρόντα νόμο, τα μέλη της Αρχής υπέχουν πειθαρχική ευθύνη. Την πειθαρχική αγωγή ασκεί ενώπιον του πειθαρχικού συμβουλίου ο Υπουργός Δικαιοσύνης για τον Πρόεδρο και τα μέλη της Αρχής και ο Πρόεδρος της Αρχής για τα μέλη της. Το πειθαρχικό συμβούλιο συντίθεται από έναν Αντιπρόεδρο του Συμβουλίου της Επικρατείας, ως πρόεδρο, έναν Αρεοπαγίτη, ένα Σύμβουλο του Ελεγκτικού Συνεδρίου και δύο Καθηγητές Α.Ε.Ι. σε γνωστικό αντικείμενο του δικαίου. Χρέη γραμματέα του συμβουλίου εκτελεί υπάλληλος της Αρχής. Ο πρόεδρος, τα μέλη και ο γραμματέας του συμβουλίου ορίζονται με ισόαριθμους αναπληρωτές. Για τα μέλη του συμβουλίου που είναι δικαστικοί λειτουργοί απαιτείται απόφαση του οικείου ανώτατου δικαστικού συμβουλίου. Το συμβούλιο συγκροτείται με απόφαση του Υπουργού Δικαιοσύνης με ισχύ επτά ετών. Το συμβούλιο συνεδριάζει με την παρουσία τεσσάρων τουλάχιστον μελών, μεταξύ των οποίων οπωσδήποτε ο πρόεδρος ή ο αναπληρωτής του, και αποφασίζει με απόλυτη πλειοψηφία των παρόντων. Σε περίπτωση ισοψηφίας υπερισχύει η ψήφος του προέδρου. Αν υπάρχουν περισσότερες από δύο γνώμες, οι ακολουθούντες την ασθενέστερη οφείλουν να προσχωρήσουν σε μία από τις επικρατέστερες. Το πειθαρχικό συμβούλιο αποφασίζει σε πρώτο και τελευταίο βαθμό την απαλλαγή ή την παύση του εγκαλουμένου. Η αμοιβή του προέδρου, των μελών και του γραμματέα του συμβουλίου καθορίζεται με κοινή απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης κατά παρέκκλιση κάθε άλλης διάταξης.

4. Μέλος της Αρχής που, κατά παράβαση του παρόντος νόμου, γνωστοποιεί με οποιονδήποτε τρόπο δεδομένα προσωπικού χαρακτήρα που είναι προσιτά σε αυτό λόγω της υπηρεσίας του ή αφήνει άλλον να λάβει γνώση αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών. Αν όμως τέλεσε την πράξη με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον αθέμιτο όφελος ή να βλάψει άλλον, επιβάλλεται κάθειρξη. Αν η πράξη του πρώτου εδαφίου τελέστηκε από αμέλεια, επιβάλλεται φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή.

Άρθρο 19
Αρμοδιότητες, λειτουργία και αποφάσεις της Αρχής

1. Η Αρχή έχει τις εξής ιδίως αρμοδιότητες:

α) Εκδίδει οδηγίες προς το σκοπό ενιαίας εφαρμογής των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

β) Καλεί και επικουρεί τα επαγγελματικά σωματεία και τις λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία δεδομένων προσωπικού χαρακτήρα στην κατάρτιση κωδίκων δεοντολογίας για την αποτελεσματικότερη προστασία της ιδιωτικής ζωής και των εν γένει δικαιωμάτων και θεμελιωδών ελευθεριών των φυσικών προσώπων στον τομέα της δραστηριότητάς τους.

γ) Απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας ή τους τυχόν εκπροσώπους τους και δίδει κατά την κρίση της δημοσιότητα σε αυτές.

δ) Χορηγεί τις άδειες που προβλέπουν οι διατάξεις του παρόντος νόμου και καθορίζει το ύψος των σχετικών παραβόλων.

ε) Καταγγέλλει τις παραβάσεις των διατάξεων του παρόντος νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.

στ) Επιβάλλει τις κατά το άρθρο 21 του παρόντος νόμου διοικητικές κυρώσεις.

ζ) Αναθέτει σε μέλος ή μέλη της τη διενέργεια διοικητικών εξετάσεων.

η) Ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους σε κάθε αρχείο. Έχει προς τούτο δικαίωμα προσβάσεως στα δεδομένα προσωπικού χαρακτήρα και συλλογής κάθε πληροφορίας για τους σκοπούς του ελέγχου, χωρίς να μπορεί να της αντιταχθεί κανενός είδους απόρρητο. Κατ' εξαίρεση, η Αρχή δεν έχει πρόσβαση στα στοιχεία ταυτότητας συνεργατών που περιέχονται σε αρχεία που τηρούνται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Τον έλεγχο διενεργεί μέλος ή μέλη της Αρχής ή υπάλληλος της Γραμματείας, ειδικά προς τούτο εντεταλμένος από τον Πρόεδρο της Αρχής. Κατά τον έλεγχο αρχείων που τηρούνται για λόγους εθνικής ασφάλειας παρίσταται αυτοπροσώπως ο Πρόεδρος της Αρχής.

θ) Γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

ι) Εκδίδει κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, στα οποία αναφέρεται ο παρών νόμος.

ια) Ανακοινώνει στη Βουλή παραβάσεις των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

ιβ) Συντάσσει κάθε χρόνο έκθεση για την εκτέλεση της αποστολής της κατά το προηγούμενο ημερολογιακό έτος. Στην έκθεση επισημαίνονται και οι τυχόν ενδεικνυόμενες νομοθετικές μεταβολές στον τομέα της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η έκθεση υποβάλλεται από τον Πρόεδρο της Αρχής στον Πρόεδρο της Βουλής και τον Πρωθυπουργό και δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως με ευθύνη της Αρχής, η οποία μπορεί να δώσει και άλλου είδους δημοσιότητα στην έκθεση.

ιγ) Εξετάζει παράπονα σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων, όταν αυτά θίγονται από την επεξεργασία δεδομένων που τους αφορούν και αιτήσεις με τις οποίες ζητείται ο έλεγχος και η εξακρίβωση της νομιμότητας των επεξεργασιών αυτών και ενημερώνει τους αιτούντες για τις σχετικές ενέργειές της.

ιδ) Συνεργάζεται με αντίστοιχες Αρχές άλλων Κρατών Μελών της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της.

2. Η Αρχή συνεδριάζει τακτικώς ύστερα από πρόσκληση του Προέδρου. Συνεδριάζει εκτάκτως ύστερα από πρόσκληση του Προέδρου ή αίτηση δύο τουλάχιστον μελών της. Οι αποφάσεις της Αρχής λαμβάνονται με πλειοψηφία τουλάχιστον τεσσάρων μελών της. Σε περίπτωση ισοψηφίας υπερισχύει η ψήφος του Προέδρου ή του αναπληρωτή του.

3. Η Αρχή καταρτίζει τον κανονισμό λειτουργίας της, με τον οποίο ρυθμίζονται ιδίως η κατανομή αρμοδιοτήτων μεταξύ των μελών της, η προηγούμενη ακρόαση των ενδιαφερομένων, θέματα πειθαρχικής διαδικασίας και ο τρόπος διεξαγωγής των κατά την περίπτωση η' της παρ. 1 του παρόντος άρθρου ελέγχων.

4. Η Αρχή τηρεί τα ακόλουθα μητρώα:

α) Μητρώο Αρχείων και Επεξεργασιών, στο οποίο περιλαμβάνονται τα αρχεία και οι επεξεργασίες που γνωστοποιούνται στην Αρχή.

β) Μητρώο Αδειών, στο οποίο περιλαμβάνονται οι άδειες που εκδίδει η Αρχή για την ίδρυση και λειτουργία αρχείων που περιέχουν ευαίσθητα δεδομένα.

γ) Μητρώο Διασυνδέσεων, στο οποίο περιλαμβάνονται οι δηλώσεις και οι άδειες που εκδίδει η Αρχή για τη διασύνδεση αρχείων.

δ) Μητρώο Προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν ως σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως.

ε) Μητρώο Αδειών Διαβίβασης, στο οποίο καταχωρίζονται οι άδειες διαβίβασης δεδομένων προσωπικού χαρακτήρα.

στ) Μητρώο Απορρήτων Αρχείων, στο οποίο καταχωρίζονται, με απόφαση της Αρχής ύστερα από αίτηση του εκάστοτε υπεύθυνου επεξεργασίας, αρχεία που τηρούν τα Υπουργεία Εθνικής Άμυνας και Δημόσιας Τάξης, καθώς και η Εθνική Υπηρεσία Πληροφοριών, για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στο Μητρώο Απορρήτων Αρχείων καταχωρίζονται και οι διασυνδέσεις με ένα τουλάχιστον αρχείο της περίπτωσης αυτής.

5. Κάθενος έχει πρόσβαση στα υπό στοιχεία α', β', γ', δ' και ε' μητρώα της προηγούμενης παραγράφου. Ύστερα από αίτηση του ενδιαφερομένου και με απόφαση της Αρχής είναι δυνατόν να επιτραπεί εν όλω ή εν μέρει η πρόσβαση και στο Μητρώο Απορρήτων Αρχείων. Ύστερα από αίτηση του υπεύθυνου επεξεργασίας ή του εκπροσώπου του και με απόφαση της Αρχής είναι δυνατόν να απαγορευθεί εν όλω ή εν μέρει η πρόσβαση στο Μητρώο Αδειών Διαβίβασης, εφόσον από αυτή θα προέκυπτε κίνδυνος για την ιδιωτική ζωή τρίτου, την εθνική ασφάλεια, τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων και την εκπλήρωση των υποχρεώσεων της χώρας που απορρέουν από διεθνείς συμβάσεις.

6. Ο Πρόεδρος εκπροσωπεί την Αρχή ενώπιον κάθε άλλης Αρχής, καθώς και σε επιτροπές και ομάδες συνεδριάσεις και συνόδους οργάνων της Ευρωπαϊκής Ένωσης, καθώς και άλλων διεθνών οργανισμών και οργάνων που προβλέπονται από διεθνείς συμβάσεις ή στις οποίες μετέχουν εκπρόσωποι αντίστοιχων Αρχών άλλων χωρών. Ο Πρόεδρος μπορεί να ανοθέτα την εκπροσώπηση της Αρχής σε μέλος της, αναπληρωτή ή και υπάλληλο του κλάδου ελεγκτών της Γραμματείας.

7. Στον Πρόεδρο της Αρχής ανήκει η ευθύνη της λειτουργίας της, καθώς και της λειτουργίας της Γραμματείας. Ο Πρόεδρος μπορεί να εξουσιοδοτεί μέλος της Αρχής ή τον προϊστάμενο της Γραμματείας ή προϊστάμενο υπηρεσίας της Γραμματείας να υπογράφει με "εντολή Προέδρου" έγγραφα, εντάλματα πληρωμής ή άλλες πράξεις. Ο Πρόεδρος είναι ο διοικητικός προϊστάμενος του προσωπικού της Γραμματείας, ασκεί την επ' αυτού πειθαρχική εξουσία και μπορεί να επιβάλλει πειθαρχική ποινή το πολύ προστίμου ίσου προς το ήμισυ των μηνιαίων αποδοχών του εγκαλουμένου.

8. Οι κανονιστικές αποφάσεις της Αρχής δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως. Οι λοιπές αποφάσεις της Αρχής ισχύουν από την έκδοση ή την κοινοποίησή τους.

9. Ένδικα βοηθήματα κατά των αποφάσεων της Αρχής μπορεί να ασκεί και το Δημόσιο. Το ένδικο βοήθημα ασκεί ο κατά περίπτωση αρμόδιος υπουργός.

10. Κάθε δημόσια αρχή παρέχει τη συνδρομή της στην Αρχή.

Άρθρο 20
Γραμματεία της Αρχής

1. Η Αρχή εξυπηρετείται από Γραμματεία. Η Γραμματεία λειτουργεί σε επίπεδο Διευθύνσεως. Η υπηρεσιακή κατάσταση των υπαλλήλων της διέπεται από τις διατάξεις που ισχύουν εκάστοτε για τους δημόσιους διοικητικούς υπαλλήλους.

2. Η οργάνωση της Γραμματείας, η διαίρεσή της σε τμήματα και γραφεία και οι επί μέρους αρμοδιότητες τούτων, ο αριθμός των θέσεων του προσωπικού κατά κλάδους και ειδικότητες και κάθε άλλη αναγκαία λεπτομέρεια καθορίζονται με προεδρικό διάταγμα, που εκδίδεται με πρόταση των Υπουργών Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, Οικονομικών και Δικαιοσύνης, ύστερα από εισήγηση της Αρχής, η οποία διατυπώνεται μέσα σε δύο (2) μήνες από τη συγκρότησή της. Με το αυτό διάταγμα προβλέπεται συγκρότηση, ως υπηρεσιακής μονάδας της Γραμματείας, τμήματος ελεγκτών, η πρόσληψη και η υπηρεσιακή κατάσταση των υπαλλήλων του οποίου ρυθμίζεται κατά παρέκκλιση από τις εκάστοτε ισχύουσες διατάξεις. Ο προϊστάμενος της Γραμματείας προέρχεται υποχρεωτικά από τον κλάδο ελεγκτών. Ο αριθμός των θέσεων του πάσης φύσεως προσωπικού της Γραμματείας δεν μπορεί να υπερβαίνει τις τριάντα (30).

3. Η πλήρωση των θέσεων της Γραμματείας γίνεται σύμφωνα με τις εκάστοτε ισχύουσες διατάξεις για την πρόσληψη δημόσιων υπαλλήλων. Ειδικά για τους υπαλλήλους του κλάδου ελεγκτών της Γραμματείας η πρόσληψή τους γίνεται από την Αρχή, με επιλογή ή διαγωνισμό, ύστερα από προκήρυξή της.

4. Τα θέματα υπηρεσιακής κατάστασης του προσωπικού της Γραμματείας κρίνονται από υπηρεσιακό συμβούλιο, που συγκροτείται με απόφαση του Προέδρου της Αρχής και αποτελείται από δύο (2) μέλη της, έναν (1) υπάλληλο που ορίζεται από αυτήν και δύο (2) αιρετούς εκπροσώπους των υπαλλήλων. Κατά τα λοιπά

εφαρμόζονται οι εκάστοτε ισχύουσες διατάξεις για τα υπηρεσιακά συμβούλια του προσωπικού των δημόσιων υπηρεσιών και των νομικών προσώπων δημοσίου δικαίου.

5. Οι τακτικοί υπάλληλοι της Γραμματείας της Αρχής υπάγονται ως προς την επικουρική ασφάλισή τους στο Ταμείο Αρωγής Προσωπικού Υπηρεσιών Αρμοδιότητος Υπουργείου Δικαιοσύνης. Όσοι προέρχονται από άλλες υπηρεσίες μπορούν να διατηρήσουν το ταμείο ασφαλίσεως της προηγούμενης υπηρεσίας τους. Οι υπάλληλοι της Γραμματείας ασφαλίζονται υποχρεωτικώς στο Ταμείο Νομικών, υπό τους αυτούς όρους με τους οποίους ασφαλίζονται και οι λοιποί έμμισθοι ασφαλισμένοι του. Οι διατάξεις της παραγράφου αυτής έχουν εφαρμογή και επί των υπαλλήλων που μετατάσσονται στη Γραμματεία της Αρχής από νομικά πρόσωπα ιδιωτικού δικαίου.

6. Κατά την πρώτη εφαρμογή του παρόντος, η πλήρωση των θέσεων προϊσταμένων υπηρεσιακών μονάδων της Γραμματείας, εκτός του Τμήματος Ελεγκτών, γίνεται ύστερα από προκήρυξη της Αρχής είτε με μετάταξη υπαλλήλων βαθμού Α΄ ή αντίστοιχου του Δημοσίου ή νομικών προσώπων δημοσίου δικαίου είτε με διορισμό. Διορισμός γίνεται μόνο στις θέσεις που δεν θα πληρωθούν με μετάταξη. Η επιλογή των μετατασσομένων ή διοριζομένων γίνεται από την Αρχή. Ο διορισμός των επιλεγομένων από την Αρχή γίνεται με απόφαση του Υπουργού Δικαιοσύνης και η μετάταξη με απόφαση του ιδίου και του οικείου υπουργού. Για τη μετάταξη δεν απαιτείται γνώμη του οικείου υπηρεσιακού συμβουλίου της υπηρεσίας από την οποία μετατάσσεται ο υπάλληλος. Τον προϊστάμενο της Γραμματείας επιλέγει η Αρχή από τους υπαλλήλους του κλάδου ελεγκτών, κατά παρέκκλιση από κάθε άλλη διάταξη.

7. Κατά την πρώτη εφαρμογή του παρόντος οι λοιπές θέσεις της Γραμματείας πληρούνται με τις προϋποθέσεις και τη διαδικασία της προηγούμενης παραγράφου. Προτιμώνται υποψήφιοι που έχουν αποδεδειγμένη εμπειρία σε θέματα πληροφορικής. Για τους υπαλλήλους του κλάδου ελεγκτών ισχύουν οι διατάξεις της παρ. 3 του παρόντος άρθρου.

8. Ο χρόνος της προηγούμενης υπηρεσίας των μετατασσομένων από νομικά πρόσωπα δημοσίου δικαίου ή νομικά πρόσωπα ιδιωτικού δικαίου λογίζεται ως χρόνος πραγματικής δημόσιας υπηρεσίας για κάθε συνέπεια.

9. Οι διατάξεις της παρ. 4 του άρθρου 18 εφαρμόζονται και επί των υπαλλήλων της Γραμματείας.

ΚΕΦΑΛΑΙΟ Ε΄
ΚΥΡΩΣΕΙΣ

Άρθρο 21
Διοικητικές κυρώσεις

1. Η Αρχή επιβάλλει στους υπευθύνους επεξεργασίας ή στους τυχόν εκπροσώπους τους τις εκάστοτε διοικητικές κυρώσεις, για παράβαση των υποχρεώσεών τους που απορρέουν από τον παρόντα νόμο και από κάθε άλλη ρύθμιση που αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα:

α) Προειδοποίηση, με αποκλειστική προθεσμία για άρση της παράβασης.

β) Πρόστιμο ποσού από τριακόσιες χιλιάδες (300.000) έως πενήντα εκατομμύρια (50.000.000) δραχμές.

γ) Προσωρινή ανάκληση άδειας.

δ) Οριστική ανάκληση άδειας.

ε) Καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή των σχετικών δεδομένων.

2. Οι υπό στοιχεία β΄, γ΄, δ΄ και ε΄ διοικητικές κυρώσεις της προηγούμενης παραγράφου επιβάλλονται πάντοτε ύστερα από ακρόαση του υπεύθυνου επεξεργασίας ή του εκπροσώπου του. Είναι ανάλογες προς τη βαρύτητα της παράβασης που καταλογίζεται. Οι υπό στοιχεία γ΄, δ΄ και ε΄ διοικητικές κυρώσεις επιβάλλονται σε περιπτώσεις ιδιαίτερα σοβαρής ή καθ' υποτροπήν παράβασης. Πρόστιμο μπορεί να επιβληθεί σωρευτικά και με τις υπό στοιχεία γ΄, δ΄ και ε΄ κυρώσεις. Εάν επιβληθεί η κύρωση της καταστροφής αρχείου, για την καταστροφή ευθύνεται ο υπεύθυνος επεξεργασίας αρχείου, στον οποίο μπορεί να επιβληθεί και πρόστιμο για μη συμμόρφωση.

3. Τα ποσά των προστίμων της παρ. 1 μπορεί να αναπροσαρμόζονται με απόφαση του Υπουργού Δικαιοσύνης, ύστερα από πρόταση της Αρχής.

4. Οι πράξεις της Αρχής με τις οποίες επιβάλλονται πρόστιμα συνιστούν εκτελεστό τίτλο και επιδίδονται στον υπεύθυνο επεξεργασίας ή τον τυχόν εκπρόσωπό του. Η εισπραξη των προστίμων γίνεται κατά τις διατάξεις του Κώδικα Εισπράξεως Δημοσίων Εσόδων (Κ.Ε.Δ.Ε.).

Άρθρο 22
Ποινικές κυρώσεις

1. Όποιος παραλείπει να γνωστοποιήσει στην Αρχή, κατά το άρθρο 6 του παρόντος νόμου τη σύσταση και λειτουργία αρχείου ή οποιαδήποτε μεταβολή στους όρους και τις προϋποθέσεις χορηγήσεως της άδειας, που προβλέπεται από την παρ. 3 του άρθρου 7 του παρόντος νόμου, τιμωρείται με φυλάκιση έως τριών (3) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

2. Όποιος κατά παράβαση του άρθρου 7 του παρόντος νόμου διατηρεί αρχείο χωρίς άδεια ή κατά παράβαση των όρων και προϋποθέσεων της άδειας της Αρχής, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

3. Όποιος κατά παράβαση του άρθρου 8 του παρόντος νόμου προβαίνει σε διασύνδεση αρχείων χωρίς να την γνωστοποιήσει στην Αρχή, τιμωρείται με φυλάκιση έως τριών (3) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών. Όποιος προβαίνει σε διασύνδεση αρχείων χωρίς την άδεια της Αρχής, όπου αυτή απαιτείται ή κατά παράβαση των όρων της άδειας που του έχει χορηγηθεί, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

4. Όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί

αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση και χρηματική ποινή και αν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) έως δέκα εκατομμυρίων (10.000.000) δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

5. Υπεύθυνος επεξεργασίας που δεν συμμορφώνεται με τις αποφάσεις της Αρχής, που εκδίδονται για την ικανοποίηση του δικαιώματος πρόσβασης, σύμφωνα με την παρ. 4 του άρθρου 12, για την ικανοποίηση του δικαιώματος αντίρρησης, σύμφωνα με την παρ. 2 του άρθρου 13, καθώς και με πράξεις επιβολής των διοικητικών κυρώσεων των περιπτώσεων γ, δ' και ε της παρ. 1 του άρθρου 21 τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών. Με τις ποινές του προηγούμενου εδαφίου τιμωρείται ο υπεύθυνος επεξεργασίας που διαβιβάζει δεδομένα προσωπικού χαρακτήρα κατά παράβαση του άρθρου 9, καθώς και εκείνος που δεν συμμορφώνεται προς τη δικαστική απόφαση του άρθρου 14 του παρόντος νόμου.

6. Αν ο υπαίτιος των πράξεων των παρ. 1 έως 5 του παρόντος άρθρου είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, ή να βλάψει τρίτον, επιβάλλεται κάθειρξη έως δέκα (10) ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

7. Αν από τις πράξεις των παρ. 1 έως και 5 του παρόντος άρθρου προκλήθηκε κίνδυνος για την εύρυθμη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή τουλάχιστον πέντε εκατομμυρίων (5.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

8. Αν οι πράξεις των παρ. 1 έως 5 του παρόντος άρθρου τελέστηκαν από αμέλεια, επιβάλλεται φυλάκιση έως τριών (3) ετών και χρηματική ποινή.

9. Για την εφαρμογή των διατάξεων του παρόντος άρθρου, αν υπεύθυνος επεξεργασίας δεν είναι φυσικό πρόσωπο, ευθύνεται ο εκπρόσωπός του νομικού προσώπου ή ο επικεφαλής της δημόσιας αρχής ή υπηρεσίας ή οργανισμού αν αυτός και ουσιαστικά τη διοικεί ή διεύθυνση αυτών.

10. Για τα εγκλήματα του παρόντος άρθρου ο Πρόεδρος και τα μέλη της Αρχής, καθώς και οι προς τούτο ειδικά εντεταλμένοι υπάλληλοι του τμήματος ελεγκτών της Γραμματείας είναι ειδικοί ανακριτικοί υπάλληλοι και έχουν όλα τα δικαιώματα που προβλέπει σχετικά ο Κώδικας Ποινικής Δικονομίας. Μπορούν να διενεργούν προανάκριση και χωρίς εισαγγελική παραγγελία, όταν πρόκειται για αυτόφωρο κακούργημα ή πλημμέλημα ή υπάρχει κίνδυνος από την αναβολή.

11. Για τα εγκλήματα της παρ. 5 του παρόντος άρθρου καθώς επίσης και σε κάθε άλλη περίπτωση όπου προηγήθηκε διοικητικός έλεγχος από την Αρχή, ο Πρόεδρος αυτής ανακοινώνει γραπτώς στον αρμόδιο εισαγγελέα οποιδήποτε αποτέλεσε αντικείμενο έρευνας από την Αρχή και διαβίβασε σε αυτόν όλα τα στοιχεία και τις αποδείξεις.

12. Η προανάκριση για τα εγκλήματα του παρόντος άρθρου περατώνεται μέσα σε δύο (2) το πολύ μήνες από την άσκηση της ποινικής δίωξης και εφόσον υπάρχουν αποχρώσες ενδείξεις για την παραπομπή του κατηγορουμένου σε δίκη, η δικάσιμος ορίζεται σε ημέρα που δεν απέχει περισσότερο από τρεις (3) μήνες από το πέρας της προανάκρισης ή αν η παραπομπή έγινε με βούλευμα δύο (2) μήνες από τότε που αυτό έγινε αμετάκλητο. Σε περίπτωση εισαγωγής της υπόθεσης με απευθείας κλήση του κατηγορουμένου στο ακροατήριο δεν επιτρέπεται η προσφυγή κατά του κλητηρίου θεσπίσματος.

13. Δεν επιτρέπεται αναβολή της δίκης για τα εγκλήματα του παρόντος άρθρου παρά μόνο μία φορά για εξαιρετικά σοβαρό λόγο. Στην περίπτωση αυτή ορίζεται ρητή δικάσιμος, η οποία δεν απέχει περισσότερο από δύο (2) μήνες και η υπόθεση εκδικάζεται κατ' εξαίρεση πρώτη.

14. Τα κακουργήματα που προβλέπονται από τον παρόντα νόμο, υπάγονται στην αρμοδιότητα του δικαστηρίου των εφετών.

Άρθρο 23
Αστική ευθύνη

1. Φυσικό πρόσωπο ή νομικό πρόσωπο ιδιωτικού δικαίου, που κατά παράβαση του παρόντος νόμου προκαλεί περιουσιακή βλάβη, υποχρεούται σε πλήρη αποζημίωση. Αν προκάλεσε ηθική βλάβη, υποχρεούται σε χρηματική ικανοποίηση. Η ευθύνη υπάρχει και όταν ο υπόχρεος όφειλε να γνωρίζει την πιθανότητα να επέλθει βλάβη σε άλλον.

2. Η κατά το άρθρο 932 Α.Κ. χρηματική ικανοποίηση λόγω ηθικής βλάβης για παράβαση του παρόντος νόμου ορίζεται κατ' ελάχιστο στο ποσό των δύο εκατομμυρίων (2.000.000) δραχμών, εκτός αν ζητήθηκε από τον ενάγοντα μικρότερο ποσό ή η παράβαση οφείλεται σε αμέλεια. Η χρηματική αυτή ικανοποίηση επιδικάζεται ανεξαρτήτως από την αιτούμενη αποζημίωση για περιουσιακή βλάβη.

3. Οι απαιτήσεις του παρόντος άρθρου εκδικάζονται κατά τα άρθρα 664-676 του Κώδικα Πολιτικής Δικονομίας, ανεξαρτήτα από την τυχόν έκδοση ή μη απόφασης της Αρχής ή την τυχόν άσκηση ποινικής δίωξης, καθώς και από την αναστολή ή αναβολή της για οποιονδήποτε λόγο. Η απόφαση του δικαστηρίου εκδίδεται μέσα σε δύο (2) μήνες από την πρώτη συζήτηση στο ακροατήριο.

ΚΕΦΑΛΑΙΟ ΣΤ'
ΤΕΛΙΚΕΣ - ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 24
Υποχρεώσεις υπεύθυνου επεξεργασίας

1. Οι υπεύθυνοι επεξεργασίας αρχείων, τα οποία λειτουργούν κατά την έναρξη ισχύος του παρόντος νόμου, υποχρεούνται να υποβάλλουν την κατά το άρθρο 6 γνωστοποίηση λειτουργίας στην Αρχή μέσα σε έξι (6) μήνες από την έναρξη λειτουργίας της Αρχής.

2. Την ίδια υποχρέωση έχουν και οι υπεύθυνοι επε-

ξεργασιες αρχειων με ευαισθητα δεδομενα, τα οποια λειτουργουν κατα την εναρξη ισχυος του παροντος νομου, προκειμενου να εκδοθει η κατα την παρ. 3 του αρθρου 7 αδεια.

3. Για αρχεια που λειτουργουν και επεξεργασιες που εκτελουνται κατα την εναρξη ισχυος του παροντος νομου οι υπευθυνοι επεξεργασιας οφειλουν να προβουν στην κατα την παρ. 1 του αρθρου 11 ενημερωση των υποκειμενων μεσα σε εξι (6) μηνες απο την εναρξη λειτουργιας της Αρχης. Η ενημερωση, εφοσον αφορα μεγαλο αριθμο υποκειμενων μπορει να γινει και δια του τυπου. Στην περιπτωση αυτη τις λεπτομερειες καθοριζει η Αρχη. Οι διαταξεις της παρ. 4 του αρθρου 11 εχουν εφαρμογη και εν προκειμενω.

4. Για τα εξ ολοκληρου μη αυτοματοποιημενα αρχεια οι προθεσμιες των προηγουμενων παραγραφων ειναι ενος (1) χρονου.

5. Οι διαταξεις των αρθρων 11, 12, 13 και 19 παρ. 1 του παροντος νομου δεν εφαρμοζονται στο περιεχομενο και στα υπηρεσιακα αρχεια που τηρουνται απο τις αρμοδιες δικαστικες αρχες για την εξυπηρετηση των σκοπων της λειτουργιας της ποινικης δικαιοσυνης και στο πλαισιο της λειτουργιας της.

Αρθρο 25
Εναρξη λειτουργιας της Αρχης

1. Μεσα σε εξηντα (60) ημερες απο την εναρξη ισχυος του παροντος νομου, διοριζεται ο Προεδρος της Αρχης και ο αναπληρωτης του. Μεσα στην ιδια προθεσμια ο Υπουργος Δικαιοσυνης υποβαλλει στον Προεδρο της Βουλης προταση για το διορισμο των τεσσαρων τακτικων μελων της Αρχης και των ισαριθμων αναπληρωτων τους.

2. Ο χρονος της εναρξης λειτουργιας της Αρχης οριζεται με αποφαση του Υπουργου Δικαιοσυνης, που εκδιδεται το αργοτερο μεσα σε τεσσερις (4) μηνες μετα τη συγκροτηση της Αρχης. Απο το διορισμο των μελων της και εως την κατα τις παρ. 6 και 7 του αρθρου 20 του παροντος νομου πληρωση των θεσεων της Γραμματειας της, η Αρχη εξυπηρετειται απο προσωπικο το οποιο αποσπαται προσωρινα σε αυτην, με αποφαση της, κατα παρεκκλιση απο καθε αλλη διαταξη.

3. Εως οτου η Αρχη λειτουργησει συμφωνα με την προηγουμενη παραγραφο, η εκκαθαριση των δαπανων της γινεται απο τη Διευθυνση Οικονομικου της Κεντρικης Υπηρεσιας του Υπουργειου Δικαιοσυνης, σε βαρος του προυπολογισμου του Υπουργειου Δικαιοσυνης.

4. Η κατα την παρ. 2 του παροντος αρθρου αποφαση του Υπουργου Δικαιοσυνης για το χρονο εναρξης λειτουργιας της Αρχης δημοσιευεται στην Εφημεριδα της Κυβερνησεως και σε τεσσερις (4) τουλαχιστον ημερησιες πολιτικες εφημεριδες ευρειας κυκλοφοριας που εκδιδονται στην Αθηνα και τη Θεσσαλονικη και σε δυο (2) τουλαχιστον ημερησιες οικονομικες εφημεριδες.

Αρθρο 26
Εναρξη ισχυος

1. Η ισχυς των διαταξεων των αρθρων 15, 16, 17, 18 και 20 του παροντος νομου αρχιζει απο τη δημοσιευση του στην Εφημεριδα της Κυβερνησεως.

2. Η ισχυς των λοιπων διαταξεων αρχιζει απο την κατα το προηγουμενο αρθρο εναρξη λειτουργιας της Αρχης.

Παραγγελλομε τη δημοσιευση του παροντος στην Εφημεριδα της Κυβερνησεως και την εκτελεση του ως νομου του Κρατους.

Αθηνα, 9 Απριλιου 1997

Ο ΠΡΟΕΔΡΟΣ ΤΗΣ ΔΗΜΟΚΡΑΤΙΑΣ
ΚΩΝΣΤΑΝΤΙΝΟΣ ΣΤΕΦΑΝΟΠΟΥΛΟΣ

Οι Υπουργοι

ΕΣΩΤΕΡΙΚΩΝ, ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΕΩΣ ΚΑΙ ΑΠΟΚΕΝΤΡΩΣΕΩΣ
ΑΛ. ΠΑΠΑΔΟΠΟΥΛΟΣ

ΕΘΝΙΚΗΣ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΟΙΚΟΝΟΜΙΚΩΝ
ΓΙΑΝΝΟΣ ΠΑΠΑΝΤΩΝΙΟΥ

ΔΙΚΑΙΟΣΥΝΗΣ
ΕΥΑΓΓΕΛΟΣ ΓΙΑΝΝΟΠΟΥΛΟΣ

ΔΗΜΟΣΙΑΣ ΤΑΞΕΩΣ
ΓΕΩΡΓΙΟΣ ΡΩΜΑΙΟΣ

ΤΥΠΟΥ ΚΑΙ ΜΕΣΩΝ ΜΑΖΙΚΗΣ ΕΝΗΜΕΡΩΣΕΩΣ
ΔΗΜΗΤΡΙΟΣ ΡΕΠΠΑΣ

Θεωρηθηκε και τεθηκε η Μεγαλη Σφραγιδα του Κρατους.

Αθηνα, 10 Απριλιου 1997

Ο ΕΠ΄ ΤΗΣ ΔΙΚΑΙΟΣΥΝΗΣ ΥΠΟΥΡΓΟΣ
ΕΥΑΓΓΕΛΟΣ ΓΙΑΝΝΟΠΟΥΛΟΣ

ΑΠΟ ΤΟ ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

Τροποποίηση των Διατάξεων του Ν.2472/97

Ημερομηνία: 8 Μαρτίου 2000 **Αριθμός φύλλου** : 84 Τεύχος Πρώτο

Άρθρο 8

Τροποποίηση των Διατάξεων του Ν.2472/97 και του Κώδικα της Πολιτικής Δικονομίας

1. Η περίπτωση α΄ της παρ.2 του άρθρου 6 του ν.2472/97 αντικαθίσταται ως εξής: α¨) Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο του και τη διεύθυνσή του. Εάν ο υπεύθυνος επεξεργασίας δεν είναι εγκατεστημένος στην ελληνική επικράτεια ή σε τόπο όπου εφαρμόζεται το ελληνικό δίκαιο, θα πρέπει επιπροσθέτως να δηλώνεται το ονοματεπώνυμο ή η επωνυμία ή ο τίτλος και η διεύθυνση του εκπροσώπου του στην Ελλάδα.¨
2. Η περίπτωση θ΄της παρ. 2 του άρθρου 6 του ν.2472/1997 διαγράφεται.
3. Η περίπτωση γ΄της παρ. 2 του άρθρου 7 του ν.2472/1997 αντικαθίσταται ως εξής: γ¨)Η επεξεργασία αφορά δεδομένα τα οποία δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου¨
4. Μετά το άρθρο 7 του ν.2472/1997 προστίθεται άρθρο $7^{α}$, το οποίο έχει ως εξής:

"Άρθρο $7^{α}$
Απαλλαγή υποχρέωσης γνωστοποίησης και λήψης άδειας

1. Ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση γνωστοποίησης του άρθρου 6 και από την υποχρέωση λήψης άδειας του άρθρου 7 του παρόντος νόμου στις ακόλουθες περιπτώσεις:

α. Όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με τη σχέση εργασίας ή έργου και είναι αναγκαία για την εκπλήρωση υποχρέωσης που επιβάλλει ο νόμος ή για την εκτέλεση της σύμβασης και το υποκείμενο έχει προηγουμένως ενημερωθεί.

β. Όταν η επεξεργασία αφορά **πελάτες ή προμηθευτές**, εφόσον τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. Για την εφαρμογή της παρούσας διάταξης τα δικαστήρια και οι δημόσιες αρχές δεν λογίζονται ως τρίτοι εφόσον τη διαβίβαση ή κοινοποίηση επιβάλλει νόμος ή δικαστική απόφαση. Δεν απαλλάσσονται από την υποχρέωση γνωστοποίησης οι ασφαλιστικές εταιρείες για όλους τους κλάδους ασφάλισης, οι φαρμακευτικές εταιρείες, οι εταιρείες εμπορίας πληροφοριών και τα χρηματοπιστωτικά νομικά πρόσωπα, όπως οι τράπεζες και οι εταιρείες έκδοσης πιστωτικών καρτών.

γ. Όταν η επεξεργασία γίνεται από **σωματεία, εταιρείες, ενώσεις προσώπων και πολιτικά κόμματα και αφορά δεδομένα τω μελών ή εταίρων τους**, εφόσον αυτοί έχουν δώσει τη συγκατάθεσή τους και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. Δεν λογίζονται ως τρίτοι τα μέλη ή οι εταίροι, εφόσον η διαβίβαση γίνεται προς αυτούς για τους σκοπούς των ως άνω νομικών προσώπων ή

ενώσεων, ούτε τα δικαστήρια και οι δημόσιες αρχές, εφόσον τη διαβίβαση επιβάλλει νόμος ή δικαστική απόφαση.

δ. Όταν η επεξεργασία γίνεται από **ιατρούς ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας και αφορά ιατρικά δεδομένα**, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από το ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει νόμος ή κώδικας δεοντολογίας και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. Για την εφαρμογή της παρούσας διάταξης τα δικαστήρια και οι δημόσιες αρχές δεν λογίζονται ως τρίτοι, εφόσον τη διαβίβαση ή κοινοποίηση επιβάλλει νόμος ή δικαστική απόφαση. Δεν εμπίπτουν στην απαλλαγή της παρούσας διάταξης τα νομικά πρόσωπα ή οι οργανισμοί που παρέχουν υπηρεσίες υγείας, όπως κλινικές, νοσοκομεία, κέντρα υγείας, κέντρα αποθεραπείας και αποτοξίνωσης, ασφαλιστικά ταμεία και ασφαλιστικές εταιρείες, καθώς και οι υπεύθυνοι επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν η επεξεργασία διεξάγεται στο πλαίσιο προγραμμάτων τηλεϊατρικής ή παροχής υπηρεσιών μέσω δικτύου.

ε. Όταν η επεξεργασία γίνεται από **δικηγόρους, συμβολαιογράφους, άμισθους υποθηκοφύλακες και δικαστικούς επιμελητές** και αφορά την παροχή νομικών υπηρεσιών προς πελάτες τους, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από υποχρέωση απορρήτου που προβλέπει νόμος και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους, εκτός από τις περιπτώσεις που αυτό είναι αναγκαίο και συνδέεται άμεσα με την εκπλήρωση εντολής του πελάτη.

2. Σε όλες τις προαναφερθείσες περιπτώσεις της παραγράφου 1 του παρόντος άρθρου, ο υπεύθυνος επεξεργασίας υπόκειται σε όλες τις υποχρεώσεις που προβλέπει ο παρών νόμος και υποχρεούται να συμμορφώνεται με ειδικούς κανόνες επεξεργασίας που η Αρχή εκδίδει σύμφωνα με την παράγραφο 3 του άρθρου 5 του παρόντος νόμου.

3. Οι **προθεσμίες** για την υποβολή γνωστοποίησης αρχείου με μη ευαίσθητα προσωπικά δεδομένα, την υποβολή αίτησης για λήψη άδειας για αρχείο με ευαίσθητα δεδομένα και για την ενημέρωση των υποκειμένων παρατείνονται **έως την 21η Ιανουαρίου 2001.**

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αλεξανδρής Ν., Κιουντουζής Ε., Τραπεζανόγλου Β., *Ασφάλεια Πληροφοριών. Τεχνικά, Νομικά και Κοινωνικά Θέματα*. Εκδ. Νέων Τεχνολογιών. Αθήνα 1995.

Γκρίτσαλης Δ., *Ασφάλεια πληροφοριακών συστημάτων σε περιβάλλοντα υψηλής ευπάθειας*, Διδακτορική Διατριβή Πανεπιστήμιο Αιγαίου, (χ.χ), http://thesis.ekt.gr/thesis/servlet/thesis?id=3188&lang=el

Γκρίτσαλης Δ., Κάτσικας Σ., Κεκλίκογλου Ι., Τομαράς Α., *Προστασία ιατρικού απορρήτου στα Πληροφοριακά Συστήματα του Εθνικού Συστήματος Υγείας*, Εκδόσεις Νέων Τεχνολογιών, Αθήνα 1990.

Khair G.M., *Σχεδίαση και υλοποίηση ασφαλών συστημάτων βάσεων δεδομένων με εφαρμογή σε πληροφοριακά συστήματα νοσοκομείων*, Διδακτορική Διατριβή Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Θεσσαλονίκη, 1996. http://thesis.ekt.gr/thesis/servlet/thesis?picPath=3-/8000-.../8911.CON&picNum=0&getPicture=Watermarke

Δρ.Διον.Γιαννακόπουλος, Δρ.Ιωαν.Παπουτσής Πληροφοριακά Συστήματα Διοίκησης Τόμος 1, Εκδόσεις "ΕΛΛΗΝ", Αθήνα 1996.

Χρ. Βασιλόπουλος, Ι. Ντόκος, Β. Σκουλάτος, Σύγχρονα Τηλεπικοινωνιακά Δίκτυα Τόμοι Α,Β,Γ,Δ, Εκδόσεις Ο.Τ.Ε. Α.Ε. – Διεύθυνση Συντήρησης, Αθήνα 2000.