IV. ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΤΗΛΕΪΑΤΡΙΚΗΣ

IV.1. ΓΕΝΙΚΑ

Η Τηλεματική προσφέρει μια εντελώς νέα προοπτική στη διαχείριση της γνώσης όσον αφορά στην απόκτησή της, τη μάθηση και τη διαβίβασή της. Είναι εύκολο να παρασυρθούν σε λάθος εκτιμήσεις οι healthcare professionals και οι ασθενείς να λάβουν λάθος θεραπεία. Η ασφάλεια και οι αξιόπιστες πληροφορίες απαιτούνται στο χώρο της περίθαλψης, ώστε οι ειδικοί να μπορούν να βασιστούν στην ορθότητα αυτών των νέου τύπου πληροφοριών.

Ένα επιπλέον ουσιώδες θέμα ασφάλειας είναι και η προστασία του απαραβίαστου του ασθενή. Και τα δύο θέματα θίγουν κυρίως ουσιώδη ζητήματα της ασφάλειας των πληροφοριακών συστημάτων ως προς την ακεραιότητα, τη διαθεσιμότητα και το απόρρητο των δεδομένων του ασθενή.

Η Ευρωπαϊκή Επιτροπή έχει ήδη εκδώσει σχετική οδηγία για την προστασία του ατόμου αναφορικά με την επεξεργασία Ατομικών Δεδομένων και την ελεύθερη διακίνηση των σχετικών δεδομένων. Συγκεκριμένα :

- Τα Εθνικά Συντάγματα αξιώνουν το σεβασμό της προσωπικής ζωής του ατόμου και του δικαιώματος της αυτοδιάθεσης των σχετικών δεδομένων.
- Η υιοθέτηση της τωρινής Κοινοτικής Οδηγίας καθοδηγεί την απαιτούμενη εναρμόνιση της εθνικής νομοθεσίας
- Η προαναφερθείσα εθνική νομοθεσία σχετίζεται με το ποινικό δίκαιο, την επαγγελματική συμπεριφορά και τη μεταφορά δεδομένων ανάμεσα σε διαφορετικά (θεραπευτικά ή ερευνητικά) ινστιτούτα.

Ο σχεδιασμός της πρότασης του Συμβουλίου της Ευρώπης «πάνω στην προστασία ιατρικών δεδομένων» στον τομέα της Υγείας χρησιμοποιώντας τηλεματική στη μεταφορά δεδομένων δεν έχει ακόμα ολοκληρωθεί και θα χρειαστούν μερικά χρόνια

ακόμα έως ότου ενσωματωθεί στην εθνική νομοθεσία. Ωστόσο οι κατευθυντήριες αρχές που ακολουθούνται είναι οι εξής :

- Έλεγχος της εισόδου μέχρι την εγκατάσταση
- Έλεγχος των μέσων δεδομένων
- Έλεγχος μνήμης
- Έλεγχος εκμετάλλευσης
- Προσπέλαση ελέγχου
- Έλεγχος επικοινωνίας
- Έλεγχος εισαγωγής δεδομένων
- Έλεγχος μεταφοράς και
- Έλεγχος διαθεσιμότητας

IV.2. ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

Όπως προαναφέρθηκε, η ασφάλεια των δεδομένων είναι μια πολύ σοβαρή υπόθεση για κάθε σύστημα που διαχειρίζεται ή διακινεί πληροφορίες, οι οποίες πολύ συχνά είναι απόρρητες ή εμπιστευτικές. Στο χώρο της διαχείρισης ιατρικών δεδομένων, τα θέματα ασφάλειας είναι συνήθως ένας μεγάλος πονοκέφαλος. Η διασφάλιση των δεδομένων πρέπει να ληφθεί υπόψη από τη φάση της σχεδίασης ακόμα ενός ιατρικού συστήματος πληροφοριών. Επίσης τα δεδομένα πρέπει να διασφαλίζονται σε κάθε στιγμή. Έτσι, σε ένα σύστημα μετάδοσης ιατρικών στοιχείων και καταχώρησης στοιχείων ιατρικού φακέλου, υπάρχουν συγκεκριμένα μέτρα που πρέπει να ληφθούν υπόψη στην αποθήκευση αλλά και στην επεξεργασία. Στις επόμενες παραγράφους παρουσιάζονται [9] γενικότερα θέματα διασφάλισης των δεδομένων σε βάσεις δεδομένων και ιατρικές ΒΔ, και θέματα μετάδοσης δεδομένων και ιατρικών δεδομένων, με σκοπό να τονίσουμε τη σημασία των θεμάτων αυτών στον κλάδο της ιατρικής πληροφορικής.

IV.2.1. Θέματα ασφάλειας βάσεων δεδομένων

Μια Βάση Δεδομένων (ΒΔ) περιέχει συνήθως πολύτιμες πληροφορίες, απαραίτητες για τη λειτουργία του οργανισμού ή της επιχείρησης στην οποία ανήκει. Είναι λοιπόν προφανές ότι η προστασία από τυχόν ατύχημα ή εσκεμμένη αλλοίωση, των πληροφοριών αυτών, αποτελεί σημαντικότατο πρόβλημα [10][11].

Οι πιθανοί κίνδυνοι που απειλούν την ασφάλεια της ΒΔ είναι πολλών μορφών. Υπάρχουν κατ' αρχήν οι φυσικές καταστροφές από φωτιά, πλημμύρες, σεισμούς κλπ, που μπορεί να συνεπάγονται απώλεια των πληροφοριών. Ακόμα και αν η ίδια η ΒΔ δεν πάθει τίποτα, είναι πολύ πιθανό σε περιπτώσεις σαν και αυτές να διακοπεί η λειτουργία της για τόσο χρόνο, ώστε να προκληθούν προβλήματα. Υπάρχουν ακόμα περιπτώσεις ανθρώπινων λαθών, όπως π.χ. να πάθει ζημιά κάποιος δίσκος κατά τη μεταφορά. Η απώλεια πληροφοριών από αμέλεια είναι επίσης πιθανή. Υπάρχουν, τέλος, κίνδυνοι για την ασφάλεια των πληροφοριών από τυχαία ή και σκόπιμη κακή χρήση του μηχανογραφικού συστήματος. Στην ενότητα αυτή, θα εξετάσουμε ιδιαίτερα τους κινδύνους που προέρχονται από την τελευταία κατηγορία, από κακή δηλαδή χρήση του μηχανογραφικού συστήματος, καθώς και τεχνικές προστασίας των ΒΔ.

IV.2.1.1 Κίνδυνοι από κακή χρήση του μηχανογραφημένου συστήματος

Οι τρεις βασικές κακές χρήσεις του μηχανογραφημένου συστήματος είναι η παράνομη απόκτηση δεδομένων, η παράνομη τροποποίηση των δεδομένων ή της δομής των δεδομένων και η παράνομη τροποποίηση των προγραμμάτων της ΒΔ.

Παράνομη απόκτηση δεδομένων

Παράνομη απόκτηση (acquisition) των δεδομένων από τη ΒΔ έχουμε όταν κάποιος χρήστης, που δεν είναι εξουσιοδοτημένος, προσπελαύνει τα δεδομένα. Εάν μάλιστα, τα δεδομένα δεν προστατεύονται (π.χ. με λέξεις κλειδιά όπως θα δούμε στη συνέχεια), τότε μπορεί να χρησιμοποιηθεί το ίδιο το σύστημα της ΒΔ για τη μη εξουσιοδοτημένη (παράνομη) προσπέλαση.

Ακόμα όμως και σε περιπτώσεις που η ΒΔ προσφέρει κάποια προστασία των δεδομένων, είναι πάλι δυνατό να αποκτήσει κάποιος μη εξουσιοδοτημένος χρήστης τα δεδομένα, γράφοντας ειδικά προγράμματα που θα προσπελάσουν απευθείας τη ΒΔ. Είναι όμως προφανής η δυσκολία κάτι τέτοιου, αφού ο παράνομος χρήστης θα πρέπει π.χ. να ανακαλύψει πρώτα τη συγκεκριμένη δομή των φυσικών αρχείων της ΒΔ.

Η παγίδευση (trapping) είναι μια ακόμη μέθοδος που χρησιμοποιείται για την παράνομη πρόσβαση σε ΒΔ από μη εξουσιοδοτημένους χρήστες. Στην περίπτωση αυτή παγιδεύονται τα σήματα ανάμεσα στον Η/Υ και κάποιο νόμιμο χρήστη, με αποτέλεσμα ο παράνομος χρήστης να αποκτά πρόσβαση στη ΒΔ χρησιμοποιώντας τους κωδικούς (εξουσιοδοτήσεις) του νόμιμου χρήστη. Η μέθοδος αυτή χρησιμοποιείται κυρίως στις περιπτώσεις που υπάρχει τηλε-επεξεργασία των δεδομένων.

Παράνομη τροποποίηση των δεδομένων

Η παράνομη τροποποίηση (modification) των δεδομένων μιας ΒΔ είναι επίσης δυνατό να γίνει με πολλούς τρόπους. Ένας από αυτούς, είναι να τροποποιηθούν παράνομα τα δεδομένα πριν καταχωρηθούν στη ΒΔ. Ένας άλλος είναι να χρησιμοποιηθεί το ίδιο το σύστημα για να κάνει τις τροποποιήσεις. Αυτό είναι δυνατό όταν δεν υπάρχει επαρκής προστασία των δεδομένων στα φυσικά αρχεία.

Ένας τρίτος τρόπος είναι να γραφούν ειδικά προγράμματα, που να τροποποιούν απ' ευθείας τα δεδομένα στα αρχεία φύλαξης τους. Τα προγράμματα όμως αυτά, είναι συνήθως περίπλοκα, μια και πρέπει να τροποποιηθεί με προσοχή, στην περίπτωση αυτή, ολόκληρη η δομή της ΒΔ (δείκτες, πίνακες κλπ.).Σε ενάντια περίπτωση, το ίδιο το σύστημα της ΒΔ θα διαγνώσει πιθανώς τη μεταβολή (π.χ. με error message).

Τέλος, παράνομη τροποποίηση των δεδομένων είναι πιθανό να γίνει με τη μέθοδο της παγίδευσης (trapping), όπως περιγράφηκε και προηγουμένως.

Παράνομη τροποποίηση των προγραμμάτων της ΒΔ

Η παράνομη τροποποίηση (modification) των προγραμμάτων μιας ΒΔ είναι η περίπτωση κατά την οποία μεταβάλλονται χωρίς εξουσιοδότηση βασικά εσωτερικά προγράμματα της ΒΔ. Μια συνηθισμένη τέτοια περίπτωση, είναι η παράνομη τροποποίηση των προγραμμάτων της ΒΔ, που εξασφαλίζουν την προστασία της μέσα από κλειδιά (passwords). Με τον τρόπο αυτό, γίνεται δυνατό να έχουν πρόσβαση στα δεδομένα της ΒΔ μη εξουσιοδοτημένοι χρήστες. Μια άλλη περίπτωση είναι να τροποποιηθούν χωρίς εξουσιοδότηση τα προγράμματα που δημιουργούν ή τυπώνουν τις πληροφορίες.

IV.2.1.2 Τεχνικές προστασίας της ΒΔ

Λέξεις κλειδιά

Οι λέξεις κλειδιά (passwords) είναι η πιο διαδεδομένη τεχνική για την προστασία της ΒΔ. Για να μπορέσει ο χρήστης να προσπελάσει δεδομένα που προστατεύονται με αυτόν τον τρόπο, θα πρέπει να δώσει πρώτα τις καθορισμένες λέξεις-κλειδιά.

Η τεχνική αυτή προστασίας μπορεί να χρησιμοποιηθεί είτε για ολόκληρη τη ΒΔ είτε για ένα μικρό υποσύνολο της, ακόμα και για ένα πεδίο κάποιας εγγραφής. Είναι δυνατό να οριστούν περισσότερες από μια τέτοιες λέξεις-κλειδιά για τα ίδια δεδομένα. Είναι ακόμα δυνατό, η προστασία αυτή να συνδεθεί με ορισμένο τύπο προσπέλασης, όπως ανάγνωση, ενημέρωση ή διαγραφή.

Σε ορισμένες περιπτώσεις, είναι χρήσιμο να οριστούν λέξεις-κλειδιά με βάση το περιεχόμενο ή κάποιο συνδυασμό δεδομένων. Για παράδειγμα, ένας χρήστης ή πρόγραμμα μπορεί να προσπελάσει κάποιο πεδίο εάν η τιμή του είναι μικρότερη από

1000. Αντίστοιχα, η προσπέλαση μπορεί να επιτρέπεται στα πεδία "επώνυμο" και "μισθός", αλλά όχι και στα δύο ταυτόχρονα.

Το κύριο πλεονέκτημα των λέξεων-κλειδιών είναι ότι εγκαθίστανται και χρησιμοποιούνται εύκολα. Το βασικό τους μειονέκτημα είναι ότι δύσκολα μπορούν να κρατηθούν μυστικά και έτσι για να είναι αποτελεσματικά πρέπει να αλλάζουν συχνά. Υπάρχει ακόμα η περίπτωση να ξεχαστούν, γι' αυτό και θα πρέπει να προβλεφθεί ένας ασφαλής τρόπος να παρακάμπτονται σε τέτοιου είδους περιπτώσεις.

Οι λέξεις-κλειδιά, τέλος, είναι αποτελεσματικές μόνο στην περίπτωση που η μη εξουσιοδοτημένη προσπέλαση επιχειρηθεί να γίνει με ανάλογο τρόπο. Αυτό είναι σημαντικό γιατί ένας συνηθισμένος τρόπος παράκαμψης της προστασίας αυτής είναι να γίνει μαζική εκτύπωση των περιεχομένων των αρχείων της ΒΔ (dumping).

Κωδικοποίηση των δεδομένων

Η κωδικοποίηση των δεδομένων (data encryption) είναι μια δεύτερη τεχνική προστασίας της ΒΔ. Με τη μέθοδο αυτή, τα δεδομένα φυλάσσονται και μεταδίδονται σε κωδικοποιημένη μορφή. Για παράδειγμα, μπορούμε να κωδικοποιήσουμε τη δυαδική απεικόνιση των δεδομένων υψώνοντας την στο τετράγωνο ή προσθέτοντας μια σταθερά.

Αλλος τρόπος κωδικοποίησης, είναι να γίνει αντιμετάθεση χαρακτήρων ή να χρησιμοποιηθεί ένα άλλο αλφάβητο. Η κωδικοποίηση των δεδομένων είναι συνήθως εύκολη στον προγραμματισμό και ιδιαίτερα αποτελεσματική σε περίπτωση παγίδευσης και παράνομης προσπέλασης με ειδικά προγράμματα. Ο τρόπος κωδικοποίησης πρέπει να φυλάγεται καλά και ο χρησιμοποιούμενος κώδικας να αλλάζει συχνά. Τα σχετικά προγράμματα κωδικοποίησης και αποκωδικοποίησης πρέπει επίσης να φυλάσσονται προσεκτικά.

Το βασικό μειονέκτημα της κωδικοποίησης είναι ότι απασχολεί σημαντικά την κεντρική μονάδα επεξεργασίας. Αυτό συμβαίνει, γιατί τα δεδομένα πρέπει να κωδικοποιούνται και να αποκωδικοποιούνται κάθε φορά που χρησιμοποιούνται. Ένας τρόπος να ξεπεραστεί το πρόβλημα είναι να κωδικοποιούνται μερικά μόνο από τα πεδία της εγγραφής, τα οποία επιλέγονται κατάλληλα. Επίσης, η κωδικοποίηση δεν παρέχει προστασία από προσπέλαση μέσω του ίδιου του συστήματος. Είναι λοιπόν

άχρηστη, αν η πρόσβαση στο σύστημα δεν προστατεύεται, π.χ. με λέξεις-κλειδιά..

Έλεγχος δραστηριότητας

Ο έλεγχος της δραστηριότητας (activity monitor), είναι ένας τρίτος τρόπος προστασίας της ΒΔ. Ο έλεγχος αυτός γίνεται με τη βοήθεια ειδικού ημερολογιακού ελέγχου (audit log), που διατηρείται από το σύστημα. Στο ημερολόγιο αυτό καταγράφονται η ημερομηνία και ο χρόνος προσπέλασης, το όνομα του προγράμματος, τα δεδομένα που προσπελάστηκαν, ο τρόπος προσπέλασης κλπ. Το ημερολόγιο αυτό πρέπει να εξετάζεται σε τακτά χρονικά διαστήματα και να διερευνώνται ιδιαίτερα οι προσπελάσεις σε ευαίσθητα δεδομένα. Υπάρχει βέβαια πάντοτε η πιθανότητα να μπορέσει κάποιος μη εξουσιοδοτημένος χρήστης, να προσπελάσει τα δεδομένα χωρίς αυτό να καταγραφεί στο ημερολόγιο. Μια μέθοδος για να ξεπεραστεί αυτό το πρόβλημα, είναι να ξαναδημιουργείται η ΒΔ κατά τακτά χρονικά διαστήματα με βάση τις εγγραφές αυτές.

Οι παραπάνω τεχνικές έχουν αποδειχτεί αποτελεσματικές σε περιπτώσεις παράνομης προσπέλασης ή τροποποίησης των δεδομένων. Δεν είναι όμως αρκετές για να προστατεύσουν το σύστημα από την παράνομη τροποποίηση των προγραμμάτων της ΒΔ. Για την αποτελεσματική προστασία τους, τα προγράμματα αυτά θα πρέπει να κρατούνται με τρόπο που να εξασφαλίζει από παράνομες παρεμβάσεις. Θα πρέπει ακόμα, να τεκμηριώνονται σχολαστικά όλες οι νόμιμες τροποποιήσεις. Το μήκος των προγραμμάτων θα πρέπει να ελέγχεται ακόμα περιοδικά, για να διαπιστώνεται αν υπάρχουν προσθήκες που δεν δικαιολογούνται από το φάκελο τεκμηρίωσης.

Εάν τέλος, τα προγράμματα έχουν αγοραστεί απευθείας από κάποιον προμηθευτή, μια καλή μέθοδος προστασίας είναι να χρησιμοποιούνται κατά διαστήματα καινούργιες κόπιες των προγραμμάτων αυτών. Με τον τρόπο αυτό, εξασφαλίζεται το ότι δεν έχει γίνει τοπική παράνομη παρέμβαση στα προγράμματα.

Μια ακόμα τεχνική για να διαπιστωθεί ότι δεν υπάρχουν παράνομες τροποποιήσεις των προγραμμάτων της ΒΔ, είναι να ελέγχονται τα προγράμματα αυτά με τη βοήθεια ενός μικρού αριθμού από test data.Siriv περίπτωση αυτή, τα αποτελέσματα συγκρίνονται με τα αναμενόμενα και τυχόν διαφορές πιθανό να σημαίνουν παράνομη παρέμβαση στα προγράμματα. Η σύγκριση αυτή είναι δυνατόν να γίνει αυτόματα, με ειδικά προγράμματα ελέγχου, αρκεί φυσικά να εξασφαλιστούν και τα ειδικά αυτά προγράμματα από παράνομες τροποποιήσεις.

Μια τελευταία τεχνική προστασίας είναι να ανατεθεί σε μια ομάδα από υπαλλήλους να προσπαθήσουν να τροποποιήσουν οι ίδιοι, με κάθε δυνατό τρόπο, "παράνομα" το σύστημα. Με τον τρόπο αυτό, μπορεί να διαπιστωθούν και να αντιμετωπιστούν τυχόν αδύνατα σημεία στις τεχνικές προστασίας της ΒΔ.

Πρέπει πάντως να παρατηρήσουμε ότι καμία τεχνική προστασίας της ΒΔ δεν είναι απολύτως ασφαλής. Η καλύτερη προστασία είναι βέβαια να μην κρατούνται πολύ ευαίσθητα δεδομένα σε ΒΔ που μπορεί να προσπελαστούν από πολλούς χρήστες.

Εάν αυτό δεν μπορεί να γίνει, πρέπει τουλάχιστον τέτοιου είδους ευαίσθητα δεδομένα να τοποθετούνται χωριστά, να γίνονται όσο το δυνατόν λιγότερα αντίγραφα και να φυλάσσονται με μεγάλη προσοχή.

IV.2.1.3 Το πρόβλημα της ταυτόχρονης προσπέλασης

Μια ΒΔ χρησιμοποιείται από πολλούς χρήστες. Είναι λοιπόν πιθανό ότι δύο ή περισσότεροι χρήστες από αυτούς θα θελήσουν να προσπελάσουν ταυτόχρονα τα ίδια δεδομένα.

Πρέπει κατ' αρχήν να διευκρινίσουμε ότι η ταυτόχρονη προσπέλαση δεν καμιά σχέση με το θέμα της ταυτόχρονης επεξεργασίας. Στα περισσότερα συστήματα υπάρχει μία μόνο κεντρική μονάδα επεξεργασίας, που υποστηρίζει τη ΒΔ. Σε ένα τέτοιο περιβάλλον, δύο ίδιες διαδικασίες δεν μπορούν να γίνουν ταυτόχρονα, παρά μόνο η μία μετά την άλλη. Βέβαια αυτό δε γίνεται τις περισσότερες φορές αντιληπτό από τον χρήστη, μια και εξωτερικά φαίνεται ότι πολλές εργασίες προχωρούν παράλληλα.

Οι δύο πιο διαδεδομένες τεχνικές για την αντιμετώπιση του προβλήματος της ταυτόχρονης προσπέλασης, είναι το "κλείδωμα" (lockout) και η "προειδοποίηση" (notification).Όταν εφαρμόζεται η τεχνική του κλειδώματος, τα δεδομένα που ζητήθηκαν για την προσπέλαση από κάποιο χρήστη Α απομονώνονται και ελέγχεται από το σύστημα η προσπέλαση από άλλους χρήστες, μέχρι να ολοκληρωθεί η διαδικασία που ζήτησε ο Α. Το κλείδωμα μπορεί να είναι δύο ειδών: αποκλειστικό (exclusive) ή προστατευτικό (protective). Αποκλειστικό κλείδωμα σημαίνει ότι απαγορεύεται η ταυτόχρονη προσπέλαση στα ίδια δεδομένα για οποιονδήποτε λόγο. Προστατευτικό κλείδωμα σημαίνει ότι επιτρέπεται η ταυτόχρονη προσπέλαση στα ίδια δεδομένα από άλλους χρήστες αλλά μόνο για ανάγνωση.

Το κλείδωμα των δεδομένων μπορεί να γίνει σε διάφορα επίπεδα. Το ανώτερο δυνατό είναι σε επίπεδο ΒΔ. Στην περίπτωση αυτή, ελέγχεται η προσπέλαση σε κάθε τμήμα της ΒΔ όπου υπάρχει ήδη προσπέλαση από κάποιο χρήστη. Το κατώτερο δυνατό είναι σε επίπεδο συγκεκριμένου πεδίου. Στην περίπτωση αυτή ελέγχεται η προσπέλαση μόνον για το συγκεκριμένο αυτό πεδίο. Υπάρχουν φυσικά και άλλα, ενδιάμεσα επίπεδα, ανάμεσα στις δύο αυτές ακραίες περιπτώσεις.

Η προειδοποίηση (notification) είναι, όπως προαναφέρθηκε, η δεύτερη τεχνική για την αντιμετώπιση του προβλήματος της ταυτόχρονης προσπέλασης. Σύμφωνα με την τεχνική αυτή, από τη στιγμή που κάποιος ζητήσει να προσπελάσει με σκοπό να τροποποιήσει ή να διαγράψει κάποιο δεδομένο, η ΒΔ αρχίζει να ελέγχει την προσπέλαση στο δεδομένο αυτό. Αν για παράδειγμα, κάποιος άλλος χρήστης ζητήσει να προσπελάσει το ίδιο δεδομένο, το σύστημα ακυρώνει την εντολή αυτή της προσπέλασης και ταυτόχρονα ειδοποιεί το δεύτερο χρήστη ότι το συγκεκριμένο δεδομένο βρίσκεται ήδη υπό προσπέλαση από κάποιον άλλο χρήστη.

IV.2.2. ΑΣΦΑΛΕΙΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΙΑΤΡΙΚΩΝ ΦΑΚΕΛΩΝ

Η ανάπτυξη πληροφοριακών συστημάτων για τον υγειονομικό κλάδο, δεν έχει τόσο προβλήματα τεχνικής φύσεως όσο νομικής, ηθικής και διαδικαστικής. Για τη σωστή σχεδίαση τέτοιων συστημάτων είναι απαραίτητη η γνώση αυτών των προβλημάτων, τα οποία θα προσπαθήσουμε να παρουσιάσουμε πολύ σύντομα.

IV.2.2.1 Προβλήματα ασφαλείας

Τα τεχνικά θέματα ασφαλείας κατά την αρχειοθέτηση πληροφοριών ιατρικού περιεχομένου δεν διαφέρουν από αυτά των υπολοίπων συστημάτων διαχείρισης δεδομένων. Έτσι, η προηγούμενη παράγραφος καλύπτει το τεχνικό μέρος της διασφάλισης των ιατρικών δεδομένων.

Ας δούμε ποια είναι τα προβλήματα που υπάρχουν κατά τη διαχείριση ιατρικών δεδομένων, και τι οφέλη υπάρχουν αντίστοιχα από τη χρήση ηλεκτρονικών ιατρικών φακέλων (Electronic Health Care Records- EHCR)[12].

- **Εξάρτηση από την τεχνολογία Η/Υ**. Η χρήση της υψηλής τεχνολογίας

διευκολύνει την επεξεργασία και τη διακίνηση των δεδομένων, αλλά παράλληλα τα EHCR στηρίζονται σε πολύ σύνθετα μηχανήματα, φαινομενικά δύσχρηστα που απαξιώνονται διαρκώς.

- **Πιστοποίηση ταυτότητας**. Κατά τη συγγραφή ενός ιατρικού φακέλου, είναι πολύ σημαντικό να πιστοποιείται ο συγγραφέας. Αυτό είναι εφικτό στα EHCR με κρυπτογραφικές μεθόδους. Αν όμως δεν εφαρμόζεται, τότε η πιστοποίηση του ιατρικού φακέλου είναι εύκολα διαβλητή. Παράλληλα δεν υπάρχει νομοθεσία που να αναγνωρίζει ως στοιχείο τα EHCR.

- **Πιστοποίηση χρήστη.** Η πιστοποίηση του χρήστη, ουσιαστικά γίνεται ελέγχοντας την πρόσβαση στα αρχεία. Με τα υπάρχοντα ανοικτά συστήματα, η χρήση λέξεων-κλειδιών δεν είναι πλέον απόλυτα ασφαλής, ενώ δεν καταχωρεί δικαιώματα χρήσης και δεν πιστοποιεί την ταυτότητα του χρήστη.

- **Ευκολία αντιγραφής.** Η χρήση Η/Υ, γενικά επιτρέπει την εύκολη αναπαραγωγή αρχείων, μειώνοντας έτσι την πιθανότητα απώλειας του πρωτοτύπου. Ωστόσο, τα αντίγραφα μπορεί να χρησιμοποιηθούν για παράνομους σκοπούς, ενώ η διασφάλιση της ακεραιότητας των δεδομένων σε πολλαπλά αντίγραφα είναι προβληματική.

- Ευκολία διακίνησης. Οι Η/Υ μπορούν να διακινούν έγγραφα από τη μία άκρη του κόσμου στην άλλη με μεγάλη ταχύτητα. Η διευρυμένη χρήση των δικτύων όμως, εγκυμονεί κινδύνους απώλειας δεδομένων, απώλειας ελέγχου διακίνησης και μειωμένης

εμπιστευτικότητας.

- Διασύνδεση δεδομένων. Οι Η/Υ, τα σχεσιακά συστήματα ΒΔ και τα δίκτυα δίνουν δυνατότητες αυξημένης πληροφόρησης. Ωστόσο, αυξάνονται και οι πιθανότητες παραβίασης του ιατρικού απορρήτου.

- Έλεγχος της πρόσβασης. Ο έλεγχος της πρόσβασης επιτρέπει τον έλεγχο των ατόμων, που έχουν πρόσβαση στη ΒΔ. Όμως, μερικές φορές, το σύστημα δεν επιτρέπει την πρόσβαση σε περιπτώσεις άμεσης ανάγκης.

- Θέματα ηθικής. Οι περισσότερες επιτροπές δεοντολογίας της Ευρώπης αποδίδουν την ευθύνη για την προστασία του ιατρικού απορρήτου στους ιατρούς, ενώ σε ιδρύματα υγειονομικής περίθαλψης, η ευθύνη αυτή αποδίδεται σε ανώτερα ιατρικά

στελέχη (π.χ. διευθυντές κλινικών).Οι περισσότεροι νόμοι δηλώνουν ότι η συλλογή ιατρικών πληροφοριών επιτρέπεται μόνο για τους σκοπούς για τους οποίους αυτές συλλέχθηκαν και σε κάθε περίπτωση ο ενδιαφερόμενος πρέπει να είναι ενήμερος και σύμφωνος. Τέλος, τα EHCR δεν είναι νομικώς κατοχυρωμένα, διότι η ηλεκτρονική μορφή της πληροφορίας είναι εύκολα αλλοιώσιμη.

IV.2.2.2 Οργάνωση συστήματος διασφάλισης των δεδομένων

Την υπευθυνότητα διαχείρισης των EHCR μοιράζονται από κοινού οι γιατροί, τα διαχειριστικά στελέχη των υγειονομικών ιδρυμάτων και οι μηχανικοί Η/Υ. Η διοίκηση και οι τεχνικοί είναι υπεύθυνοι για τη συντήρηση του πληροφοριακού συστήματος και τη διασφάλιση των δεδομένων του. Θεωρητικά, η βέλτιστη λύση για τη διασφάλιση των δεδομένων, τη δημιουργία και εφαρμογή πρωτοκόλλων καλής συμπεριφοράς και χρήσης των πληροφοριών, θα πρέπει να αποδοθεί σε μια ανεξάρτητη διοικητικά και οικονομικά αρχή. Στην πράξη όμως η δημιουργία μιας ομάδας ασφάλειας δεδομένων (ΟΑΔ) είναι πιο ρεαλιστική. Η ΟΑΔ αποτελείται από υψηλόβαθμα ιατρικά στελέχη, διοικητικό προσωπικό, μηχανικούς Η/Υ και ειδικούς σε θέματα ασφάλειας δεδομένων, Η ομάδα αυτή προετοιμάζει, σχεδιάζει και επιβλέπει την εφαρμογή της πολιτικής διαχείρισης δεδομένων. Επίσης, είναι υπεύθυνη για την παρακολούθηση της εσωτερικής και διεθνούς νομοθεσίας, για την εφαρμογή αρχών προστασίας δεδομένων, για την αναγνώριση των πιθανών κινδύνων και την εφαρμογή των τελευταίων τεχνικών λύσεων. Επίσης, η ομάδα αυτή είναι επιφορτισμένη με την εκπαίδευση του προσωπικού σε θέματα ασφάλειας και Η/Υ. Η ομάδα αυτή πρέπει να λογοδοτεί σε μια συμβουλευτική επιτροπή σε θέματα πληροφοριών.

IV.3. ΑΣΦΑΛΕΙΑ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΥΓΕΙΟΝΟΜΙΚΗΣ ΠΕΡΙΘΑΛΨΗΣ

IV.3.1 Κλειστά και ανοικτά συστήματα

Τα πληροφοριακά συστήματα μπορούν να χωριστούν σε κλειστά και ανοικτά συστήματα [13]. Τα κλειστά, είναι αυτά τα οποία δεν επικοινωνούν με άλλα συστήματα πληροφοριών. Η ασφάλεια σε τέτοια συστήματα είναι ευκολότερη.

Τα ανοικτά συστήματα, αντίθετα, είναι πιο πολύπλοκα και συνεπώς η διασφάλιση των δεδομένων είναι πιο δύσκολη. Τα συστήματα αυτά είναι ένα σύνολο διασυνδεόμενων υποσυστημάτων, τα οποία έχουν χωριστές λειτουργικότητες και κανόνες ασφάλειας.

IV.3.2 Ασφάλεια σε τηλεϊατρικά δίκτυα και στη μετάδοση δεδομένων γενικότερα

Τα ανοικτά συστήματα υγειονομικής περίθαλψης είναι πάντα δικτυακές εφαρμογές. Έτσι, μια από τις κύριες εργασίες τους είναι η μετακίνηση δεδομένων μέσω τηλεπικοινωνιακών δικτύων είτε αυτά είναι εσωτερικά μέσα σε ένα ίδρυμα είτε είναι εξωτερικά, με τη χρήση μισθωμένων γραμμών, ου απλού τηλεφωνικού δικτύου, του δικτύου ISDN ή άλλα. Κατά συνέπεια έχουν τους ίδιους κανόνες ασφαλείας με τα συστήματα των τηλεϊατρικών εφαρμογών. Μπορούμε λοιπόν να εξετάσουμε ταυτόχρονα τις απαιτήσεις ασφαλείας. Αυτές κυρίως είναι απαιτήσεις ασφαλείας κατά τη διακίνηση δεδομένων.

IV.3.2.1 Απειλές ασφάλειας

Τα προβλήματα ασφάλειας ενός τηλεπικοινωνιακού συστήματος έχουν αναγνωριστεί από τη διεθνή συμβουλευτική επιτροπή τηλεγράφων και τηλεφώνων (Comite Consulatif International Telegrafique et Telephonique - CCITT) και είναι τα παρακάτω [13].

- **Ανάσχεση ταυτότητας:** δηλαδή υποκλοπή των στοιχείων ταυτότητας για παράνομους σκοπούς.
- **Μεταμφίεση:** ένας χρήστης χρησιμοποιεί τη ταυτότητα ενός άλλου χρήστη για να καρπωθεί τα δικαιώματα πρόσβασης άλλου.
- **Επαναχρησιμοποίηση** μηνύματος το οποίο έχει υποκλαπεί

• **Ανάσχεση δεδομένων:** ένας μη εξουσιοδοτημένος χρήστης αποκτά πληροφορίες κατά τη διάρκεια μιας συνδιάλεξης

• **Τροποποίηση πληροφοριών:** οποιαδήποτε αλλαγή, καταστροφή ή προσθήκη στα δεδομένα

• **Αποκήρυξη (repudiation):** ένας χρήστης αρνείται ότι συμμετείχε σε κάποια επικοινωνία

• **Αρνηση παροχής υπηρεσιών:** κάποιος παρεμποδίζει η μπλοκάρει τη μετάδοση δεδομένων, κυρίως στις κρίσιμες στιγμές.

• **Λάθος δρομολόγηση δεδομένων:** δεδομένα που είχαν άλλο προορισμό τελικά παραδόθηκαν σε άλλο χρήστη

• **Ανάλυση τηλεπικοινωνιακής κίνησης:** κάποιος συλλέγει χωρίς άδεια πληροφορίες για τη χρήση ενός δικτύου, τη παρουσία συγκεκριμένων χρηστών κλπ.

Συνεπώς κατά τη χρήση τηλεπικοινωνιακών συστημάτων υπάρχουν τέσσερα βασικά προβλήματα : η παραβίαση, η πιστοποίηση ταυτότητας, η εμπιστευτικότητα και η διαχείριση δεδομένων.

IV.3.2.2 Απαιτήσεις ασφάλειας

Μια ιδανική λύση για ασφαλή επικοινωνία ικανοποιεί τις παρακάτω βασικές απαιτήσεις:

* **Εμπιστευτικότητα (confidentiality):** όλες οι επικοινωνίες περιορίζονται μόνο στα εμπλεκόμενα μέρη. Η εμπιστευτικότητα είναι ένα βασικό στοιχείο της απομόνωσης του χρήστη, της προστασίας ιατρικών πληροφοριών καθώς και ένα εμπόδιο στη υποκλοπή πληροφοριών.

* **Πιστοποίηση (authentication):** και τα δύο μέρη πρέπει να ξέρουν ότι επικοινωνούν με το ορθό μέρος. Η πιστοποίηση παρέχεται συνήθως με την χρήση ψηφιακών υπογραφών και πιστοποιητικών.

• **Ακεραιότητα δεδομένων (integrity):** τα δεδομένα που έχουν σταλεί ως μέρος μιας συναλλαγής, δεν πρέπει να επιδέχονται τροποποιήσεις κατά την μεταφορά τους, Ομοίως, δεν θα πρέπει να τροποποιηθούν τα δεδομένα ούτε κατά τη διάρκεια της αποθήκευσης τους.

- **Μη δυνατότητα αποκήρυξης (non repudiation):** κανένα μέρος δεν πρέπει να μπορεί να αρνηθεί ότι έχει συμμετάσχει σε συναλλαγή μετά τη διεξαγωγή της.

Η εμπιστευτικότητα συνήθως παρέχεται με την κρυπτογράφηση . Η πιστοποίηση, η ακεραιότητα των δεδομένων και μη δυνατότητα αποκήρυξης συνήθως παρέχονται με την χρήση ψηφιακών υπογραφών και δημοσίων κωδικών κλειδιών. Αυτές οι τέσσερις απαιτήσεις είναι βασικές και πρέπει να ισχύουν σε κάθε στιγμή.

IV.3.2.3 Κρυπτογράφηση

Σε γενικές γραμμές κρυπτογράφηση είναι η κατάλληλη μετατροπή ενός μηνύματος (αρχείου ή τμήματος αυτού) έτσι που να αποκρύπτεται το περιεχόμενο του [14]. Οι αλγόριθμοι που χρησιμοποιούνται για την κρυπτογράφηση λέγονται Cipher, ένα κρυπτογραφημένο κείμενο ονομάζεται cyphertext Αντίθετα η διαδικασία της ανάγνωσης κρυπτογραφημένου μηνύματος ονομάζεται αποκρυπτογράφηση.

Οι αλγόριθμοι κρυπτογράφησης (Cipher) είναι οι μαθηματικές συναρτήσεις οι οποίες χρησιμοποιούνται για την κρυπτογράφηση και για την αποκρυπτογράφηση μηνυμάτων (γενικά χρησιμοποιούνται δυο συναρτήσεις, μία για κρυπτογράφηση και μια για αποκρυπτογράφηση).

Όταν η ασφάλεια ενός αλγορίθμου βασίζεται στην μυστικότητα του τότε ο αλγόριθμος αυτό ονομάζεται απαγορευμένος αλγόριθμος. Οι αλγόριθμοι αυτοί έχουν χρησιμοποιηθεί από την αρχή της κρυπτογραφίας αλλά είναι κάτι πολύ δύσκολο στο να εφαρμοστεί. Εάν για παράδειγμα ένας τέτοιος αλγόριθμος χρησιμοποιείται από μια μεγάλη ομάδα ανθρώπων τότε, όταν ένας από όλους αναγκαστεί να φύγει πρέπει όλη η ομάδα να χρησιμοποιεί καινούργιο.

Οι μοντέρνες μέθοδοι κρυπτογραφίας δεν χρησιμοποιούν απαγορευμένους αλγόριθμους αλλά αλγόριθμους με την χρήση κλειδιού. Το κλειδί είναι συγκεκριμένου μεγέθους μήνυμα το οποίο χρησιμοποιείται και στη συνάρτηση κρυπτογράφησης και στην συνάρτηση αποκρυπτογράφησης (είναι και οι δυο συναρτήσεις εξαρτημένες από την τιμή αυτού του κλειδιού):

Επιλογή αλγορίθμου

Εμπλέκονται διάφορα ζητήματα κατά την επιλογή κατάλληλου αλγόριθμου κρυπτογράφησης:

• Μπορεί να επιλέγει ένας δημοσιευμένος αλγόριθμος. Αυτό βασίζεται στην λογική ότι ένας δημόσιος αλγόριθμος έχει αξιολογηθεί από διάφορους, εάν κανείς δεν έχει καταφέρει να παραβιάσει την ασφάλεια του τότε είναι αρκετά καλός αλγόριθμος.

• Εμπιστοσύνη σε κατασκευαστή. Αυτό βασίζεται στο γεγονός ότι ένας κατασκευαστής με φήμη στο χώρο δεν πρόκειται να δώσει η να πουλήσει αλγόριθμο προτού γίνει διεξοδικός έλεγχος για την ασφάλεια του.

• Εμπιστοσύνη σε ιδιωτικό συμβουλευτικό οργανισμό. Αυτό βασίζεται ότι ο ιδιωτικώς οργανισμός είναι κατάλληλα εξοπλισμένος για να αξιολογήσει και να προτείνει κάποιο αλγόριθμο.

• Εμπιστοσύνη σε κυβερνητικούς οργανισμούς. Βασιζόμενη στην αξιοπιστία ενός κυβερνητικού φορέα.

• Συγγραφή αλγόριθμου. Ο χρήστης μπορεί να δημιουργήσει δικούς του αλγόριθμους κρυπτογράφησης.

Για όλα τα πιο πάνω υπάρχουν διάφορα προβλήματα, το πρώτο είναι το πιο αξιόπιστο. Η εμπιστοσύνη σε ένα και μόνο κατασκευαστή η σε κυβερνητικούς φορείς είναι κάτι πολύ επίφοβο, το οποίο και δεν μπορεί να εγγυηθεί τίποτα. Η εμπιστοσύνη σε ιδιωτικό φορέα πάλι εγκυμονεί κινδύνους γιατί κανένας δεν μπορεί να θεωρηθεί αυθεντία στο χώρο, το ίδιο γίνεται και με την συγγραφή αλγορίθμων από τον χρήστη. Οι αλγόριθμοι οι οποίοι είναι ήδη δημοσιευμένοι και αξιολογημένοι είναι ίσως η καλύτερη λύση, ειδικά όταν ένας αλγόριθμος έχει αξιολογηθεί από πολλούς και τα αποτελέσματα είναι δημοσιευμένα.

IV.3.2.4 Ψηφιακές υπογραφές

Η ψηφιακή υπογραφή είναι ένα ασύμμετρο κρυπτογραφικό εργαλείο[65]. Επιτρέπει τη μεταφορά των πλεονεκτημάτων των απλών χειρόγραφων υπογραφών στους Η/Υ. Αυτά τα πλεονεκτήματα είναι:

• Ότι μόνο ο ιδιοκτήτης μπορεί να παράγει τη συγκεκριμένη υπογραφή

• Η πλαστογράφηση είναι συνήθως πολύ δύσκολη

• Η υπογραφή είναι αναγνωρίσιμη

Ψηφιακή υπογραφή είναι η κρυπτογράφηση ενός κειμένου με ένα προσωπικό κλειδί,

χρησιμοποιώντας όλα τα bits του αρχείου. Έτσι κάθε αλλαγή του αρχικού κειμένου αλλάζει τη ψηφιακή υπογραφή. Η βεβαίωση της υπογραφής γίνεται με ένα δεύτερο δημόσιο κλειδί που αντιστοιχεί στο προσωπικό κλειδί και αποστέλλεται μαζί με το κείμενο.

Επειδή η υπογραφή με όλα τα bits ενός αρχείου είναι χρονοβόρα διαδικασία, έχουν υλοποιηθεί συστήματα που συμπιέζουν ένα αρχείο σε ένα άλλο σταθερού μεγέθους και στη συνέχεια υπογράφεται αυτό το ενδιάμεσο αρχείο. Η συμπίεση γίνεται με συναρτήσεις "hash functions" οι συναρτήσεις αυτές είναι γνωστές σε όλα τα εμπλεκόμενα μέρη.

IV.4. ΝΟΜΙΚΑ ΘΕΜΑΤΑ ΙΑΤΡΙΚΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τα νομικά ζητήματα που προκύπτουν στην ιατρική πληροφορική είναι πολλά και καλύπτουν ένα ευρύ φάσμα νομικών αρχών. Το πρόβλημα γίνεται ακόμα εντονότερο, με τα κενά που υπάρχουν τόσο στις εθνικές όσο και στη διεθνή νομοθεσία. Κάποιες οδηγίες υπάρχουν και είναι "οι οδηγίες για την ασφάλεια πληροφοριακών συστημάτων" του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης ("the OECD Guidelines for the security of information systems") του 1992, "Η απόφαση του συμβουλίου της Ευρωπαϊκής Ένωσης στο θέμα της ασφάλειας των πληροφοριακών συστημάτων", το 1992 ("EU Council Decision in the field of Security of Information Systems"), το πρωτόκολλο 108 του Συμβουλίου της Ευρώπης (COE Convention 108) και "ο/ οδηγίες τον SEISMED" (Secure environment for information systems in medicine), που υλοποιήθηκαν για το κοινοτικό πρόγραμμα AIM (Advanced informatics in medicine), το 1991.

Σημαντική συμβολή στο όλο θέμα, θα έχει η κοινοτική οδηγία για την προστασία των ατόμων σε σχέση με την επεξεργασία προσωπικών τους στοιχείων και την ελεύθερη διακίνηση αυτών των στοιχείων “EU Directive 95/EC of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and of the free movement of such data"}, η οποία ψηφίστηκε στις 20 Φεβρουαρίου του 1995 [15].

Αναλυτικότερα [16] :

IV.4.1. Ασφάλεια δεδομένων

Η νομοθεσία θα πρέπει να είναι σε θέση να διασφαλίζει το ιατρικό απόρρητο των ασθενών και να εγγυάται την ιατρική εμπιστευτικότητα. Έτσι, οι αρχές προστασίας των δεδομένων

είναι οι ακόλουθες:

- προστασία των προσωπικών στοιχείων προστασία ιατρικών δεδομένων
- πολλαπλά επίπεδα ασφάλειας
- τήρηση των δικαιωμάτων των ανθρώπων, οι οποίοι έχουν αρχειοθετημένα στοιχεία
- έλεγχος στη ροή και διακίνηση των δεδομένων

IV.4.2. Ασφάλεια πληροφοριακών συστημάτων

Η ασφάλεια των πληροφοριακών συστημάτων, όπως έχει τονιστεί και προηγουμένως, χωρίζεται σε τέσσερα επίπεδα ασφάλειας:

- επίπεδο συστημάτων
- επίπεδο πρόσβασης
- επίπεδο επικοινωνίας
- επίπεδο αρχειοθέτησης

Η τήρηση των αρχών, που έχουν παρουσιαστεί στις προηγούμενες παραγράφους, καλύπτει και διασφαλίζει πλήρως ένα πληροφοριακό σύστημα.

IV.4.3. Νομική αναγνώριση ψηφιακών δεδομένων

Η χρήση πληροφοριακών συστημάτων εκμηδενίζει τη χρήση παραδοσιακών εγγράφων. Ένα πρόβλημα είναι η αναγνώριση στοιχείων και εγγράφων, που προέρχονται από ένα τέτοιο σύστημα, από δικαστήρια ως νόμιμα πειστήρια, Η ευκολία με την οποία μπορούν να καταστραφούν ή να αλλοιωθούν αυτά τα στοιχεία, τα καθιστά αναξιόπιστα.

Η υπάρχουσα νομοθεσία είναι ανεπαρκής και η νομική αναγνώριση των ψηφιακών δεδομένων ποικίλει ανάλογα με τη χρήση των εγγράφων αυτών.

IV.4.4. Υπευθυνότητα

Το θέμα της υπευθυνότητας και της αποδοχής των ευθυνών του κάθε εμπλεκόμενου στον ιατρικό κλάδο, είναι ένα πολύπλοκο θέμα από μόνο του. Η εμπλοκή των πληροφοριακών συστημάτων δημιουργεί ένα ακόμα πιο σύνθετο πλαίσιο σχέσεων, αφού στη γνωστή σχέση ιατρού - ασθενή προστίθεται και η σχέση ανθρώπου - μηχανής. Πάντως, σε καμιά περίπτωση η ύπαρξη των συστημάτων αυτών δεν μειώνει το ποσοστό ευθύνης τους κατά την εργασία τους. Αντίθετα, όσο μεγαλύτερη είναι η ανάμειξη τους με τους Η/Υ, τόσο αυξάνονται οι ευθύνες. Αυτός είναι και ένας από τους λόγους, για τους οποίους τα συστήματα αυτά δεν είναι πάντα αποδεκτά από το ιατρικό προσωπικό.

Ωστόσο, το ιατρικό προσωπικό δεν αναλαμβάνει την ευθύνη για οποιοδήποτε πρόβλημα. Οι διαχειριστές των συστημάτων αναλαμβάνουν την ευθύνη της καλής λειτουργίας των συστημάτων ενώ οι μηχανικοί ανάπτυξης εφαρμογών πρέπει να λαμβάνουν σοβαρά υπόψη ποιοι θα είναι οι τελικοί χρήστες των προϊόντων τους, αφού αυτοί έχουν την ευθύνη για τυχόν δυσλειτουργίες του συστήματος.

IV.4.5. Πνευματικά δικαιώματα

Η τήρηση των πνευματικών δικαιωμάτων είναι πολύ δύσκολη. Το θέμα αυτό είναι σε πλήρη αντιστοιχία με τα θέματα των πνευματικών δικαιωμάτων των εταιρειών λογισμικού.

IV.5. ΟΔΗΓΙΕΣ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΑΣΦΑΛΩΝ ΕΦΑΡΜΟΓΩΝ ΙΑΤΡΙΚΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

IV.5. 1. Ασφαλής σχεδίαση

Μια ασφαλής σχεδίαση περιλαμβάνει τέσσερα στάδια [17] :

1. το στάδιο σχεδίασης της διαχείρισης του έργου. Σε αυτή τη φάση υπολογίζονται και καταγράφονται οι ανάγκες της εφαρμογής, τα θέματα ασφάλειας που προκύπτουν και τα υποσυστήματα της προστασίας των δεδομένων. Επίσης καταγράφονται οι ευθύνες των εμπλεκόμενων μερών, τόσο στη σχεδίαση όσο και στην υλοποίηση, ενώ αναλύονται οι ανάγκες εκπαίδευσης του προσωπικού στην εφαρμογή.

2. το στάδιο της ανάπτυξης της εφαρμογής. Δημιουργείται καταρχήν, ένα προσχέδιο ποιότητας (quality plan). Με βάση αυτό το σχέδιο, ακολουθείται η διαδικασία του εντοπισμού της κεντρικής ιδέας, της μελέτης των απαιτήσεων, του αρχικού σχεδιασμού, της κωδικοποίησης και-τεμαχισμού της εργασίας και της ολοκλήρωσης των επιμέρους συστημάτων.

3. το στάδιο της σχεδίασης. Σε αυτή τη φάση πρέπει να λαμβάνονται υπ' όψιν: η μείωση της πολυπλοκότητας του συστήματος, ο έλεγχος της αρχιτεκτονικής της εφαρμογής, η χρήση δομημένου προγραμματισμού, η μοντελοποίηση των δεδομένων και η ανίχνευση λαθών.

4. το στάδιο επιλογής του περιβάλλοντος ανάπτυξης της εφαρμογής. Κατά τη φάση επιλογής της γλώσσας προγραμματισμού, πρέπει να λαμβάνονται υπόψη ότι η γλώσσα πρέπει να είναι συμβατή με την εφαρμογή, όλα τα σφάλματα πρέπει να είναι εντοπίσιμα, πρέπει να ακολουθηθεί το αρχικό μοντέλο σχεδίασης και η γλώσσα δεν πρέπει να έχει ασάφειες.

IV.5.2. Ασφαλής υλοποίηση

Η υλοποίηση αφορά σε όλες τις ενέργειες που πρέπει να γίνουν μετά την ολοκλήρωση της ανάπτυξης της εφαρμογής. Έτσι, οι ενέργειες αυτές είναι η μεταφορά του προγράμματος από το ιδανικό περιβάλλον του προγραμματιστή στο προς διαμόρφωση περιβάλλον του τελικού χρήστη και η τελική διαμόρφωση του, ώστε να λειτουργεί κανονικά. Πριν την υλοποίηση πρέπει να καθοριστούν οι

απαιτήσεις των τελικών χρηστών, να δημιουργηθεί ένα πλάνο ασφαλούς υλοποίησης και να σχεδιαστεί ένα πλάνο αναγκών υλικού (hardware).

Η φάση της υλοποίησης, μπορεί να χωριστεί στα παρακάτω:

- Εγκατάσταση των αρχείων στο χώρο υποδοχής
- Πειραματική λειτουργία
- Εφαρμογή αλλαγών που θα προκύψουν από την πειραματική λειτουργία
- Παρουσίαση της εφαρμογής στο αρμόδιο προσωπικό. Επίσης, σε αυτή τη φάση θα γίνει η διερεύνηση της υποδομής του προσωπικού, ενημέρωση του προσωπικού, δοκιμαστική λειτουργία της εφαρμογής από το προσωπικό, αξιολόγηση του συστήματος από το προσωπικό και εκπαίδευση του προσωπικού για τις απαιτήσεις του συστήματος.
- Τελική λειτουργία της εφαρμογής.