

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή

στα Πληροφοριακά και Επικοινωνιακά Συστήματα



Ηλεκτρονική Υγεία και Ηλεκτρονικός Φάκελος

Λορέντο Γκούρη

Επιβλέπων Καθηγητής
Δρ. Αντώνης Μ. Χατζηαντώνης

Μάιος 2014

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ηλεκτρονική Υγεία και Ηλεκτρονικός Φάκελος



Λοέλντο Γκούρη

Επιβλέπων Καθηγητής
Δρ. Αντώνης Μ. Χατζηαντώνης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2014

Περίληψη

Τα πληροφοριακά και επικοινωνιακά συστήματα έχουν εισχωρήσει στον χώρο της υγείας καθώς σταδιακά αντικαθιστούν τα παραδοσιακά συστήματα συλλογής και αποθήκευσης πληροφοριών, τα οποία βασίζονταν σε χειρόγραφους φακέλους ασθενών. Όμως, η ευκολία με την οποία τα δεδομένα μπορούν να επεξεργαστούν σε ένα πληροφοριακό σύστημα υγείας και ιδιαίτερα σε ένα σύστημα διαχείρισης ηλεκτρονικών φακέλων ασθενών, δημιουργεί ζητήματα που άπτονται στο δικαίωμα της ιδιωτικότητας.

Στόχος της παρούσας εργασίας είναι η διερεύνηση των ζητημάτων αυτών και η ανάλυση της τρέχουσας κατάστασης στον τομέα των πληροφοριακών συστημάτων υγείας δίνοντας έμφαση σε τέσσερις κύριους άξονες: στο νομικό πλαίσιο λειτουργίας αυτών στην Ελλάδα και την Ευρωπαϊκή Ένωση, στις προσπάθειες προτυποποίησης και τέλος στις τεχνολογικές εξελίξεις των τελευταίων ετών στην παγκόσμια βιβλιογραφία σχετικά με την προστασία της ιδιωτικότητας στο χώρο των πληροφοριακών συστημάτων υγείας και ιδιαίτερα των συστημάτων διαχείρισης ηλεκτρονικών φακέλων ασθενών.

Στη συνέχεια, όλοι οι παραπάνω τομείς αξιολογούνται σε μια προσπάθεια εξαγωγής συμπερασμάτων σχετικά με την επάρκεια και την αποτελεσματικότητά τους όσον αφορά στην προστασία της ιδιωτικότητας των ασθενών. Τα συμπεράσματα αυτά καθώς και προτάσεις για περαιτέρω έρευνα παρουσιάζονται στο τελευταίο μέρος της εργασίας.

Summary

Information and communication systems have spread in the field of health while they gradually replace traditional collecting and storing information systems, which are based on hand written patient files. Nevertheless the ease provided to edit this data in an health information system and particular in a system created to manage electronic patient records, comes with issues closely related to the right in privacy.

This thesis tries to investigate these issues and to analyse the current situation in the field of health information systems, emphasising four main aspects: their operating legal framework in Greece and the European Union, the attempts of prototyping such systems and the technological developments of the latest years in bibliography having to do with the protection of privacy regarding health information systems and specifically electronic patient records management systems. All these fields are being evaluated in an attempt to conclude on the sufficiency, adequacy and efficiency of these systems, as far as patients' privacy preservation is concerned. These results and suggestions for future research are being noted in the last part of this thesis.

Ευχαριστίες

Υπεύθυνος καθηγητής της διπλωματικής μου εργασίας ήταν ο Δρ. Αντώνης Χατζηαντώνης, τον οποίο θα ήθελα να ευχαριστήσω για την βοήθεια, ενδιαφέρον και καθοδήγηση του κατά τη διάρκεια της δουλειάς μου. Πάνω απ' όλα, είμαι ευγνώμων στους γονείς μου για την ολόψυχη αγάπη και υποστήριξή τους όλα αυτά τα χρόνια. Αφιερώνω αυτή την εργασία σε αυτούς και στο στενό μου περιβάλλον το οποίο βρίσκεται πάντα δίπλα μου.

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή	5
Κεφάλαιο 1	6
Νέες Τεχνολογίες και Υγεία	6
1.1 Η Έννοια της Πληροφορίας	6
1.1.1 Πληροφορία στην Επιχείρηση	8
1.1.2 Γνώση στην Επιχείρηση	8
1.2 Η Αξία των Νέων Τεχνολογιών	9
1.3 Η Έννοια των Πληροφοριακών Συστημάτων	10
1.3.1 Ορισμός	10
1.3.2 Συστατικά Μέρη Πληροφοριακού Συστήματος	12
1.4 Ηλεκτρονική Υγεία (e-Health)	15
1.5 Πληροφοριακά Συστήματα υγείας	16
1.5.1 Συστήματα Υγείας και Πληροφορική	18
1.5.2 Ιατρικά Πληροφοριακά Συστήματα	19
1.5.3 Πληροφορική και Υγεία	20
Κεφάλαιο 2	21
Ηλεκτρονικός Φάκελος	21
2.1 Η Έννοια του Ηλεκτρονικού Φακέλου Υγείας	21
2.2 Δομή Ηλεκτρονικού Φακέλου Υγείας	24
2.2.1 Στοιχειώδης Πληροφορία (Item)	24
2.2.2 Επαφή (Contact), Επεισόδιο (Episode)	25
2.2.3 Ιατρικές, Διαχειριστικές Πληροφορίες (Medical, Administrative Information)	26

2.3 Συστήματα Ηλεκτρονικού Φακέλου Υγείας	27
2.4 Χρήσεις Ηλεκτρονικού Φακέλου Υγείας	28
2.5 Πλεονεκτήματα - Μειονεκτήματα Ηλεκτρονικού Φακέλου Υγείας	30
Κεφάλαιο 3	35
Ασφάλεια και Νομοθετικό Πλαίσιο	35
3.1 Ασφάλεια Ηλεκτρονικού Φακέλου Υγείας	35
3.1.1 Απειλές Πληροφοριακών Συστημάτων Υγείας	35
3.1.2 Απειλές Πληροφοριακών Συστημάτων Υγείας	37
3.1.2.1 Δέκα Βήματα για Ασφάλεια Πληροφοριακών Συστημάτων Υγείας	37
3.1.3 Ασφάλεια Ηλεκτρονικού Ιατρικού Φακέλου	40
3.2 Ιδιωτικότητα, Εμπιστευτικότητα, Ακεραιότητα Ηλεκτρονικού Φακέλου Υγείας	41
3.2.1 Απαιτήσεις Ασφάλειας	41
3.2.2 Εμπιστευτικότητα (Confidentiality)	41
3.2.3 Ακεραιότητα (Integrity)	44
3.2.4 Αυθεντικοποίηση (Authentication)	47
3.2.5 Εξουσιοδότηση (Authorization)	48
3.2.6 Ανωνυμία (Anonymity)	49
3.2.7 Μη Αποποίηση (Non Repudation)	49
3.2.8 Καταγραφή Γεγονότων (Auditing)	50
3.2.9 Ενοποίηση Δεδομένων (Data Aggregation)	51
3.3 Νομοθετικό Πλαίσιο	52
3.3.1 Ελλάδα	52
3.3.1.1 Νόμος 2472/1997	52

3.3.1.2 Νόμος 3471/2006	57
3.3.1.3 Νόμος 3418/2005	63
3.3.2 Ευρωπαϊκή Ένωση	65
3.3.2.1 Οδηγία 95/46/EK	66
3.3.2.2 Οδηγία 2002/58/EK	67
3.3.2.3 Οδηγία 2006/24/EK	70
Συμπεράσματα	72
Βιβλιογραφία	76

ΕΙΣΑΓΩΓΗ

Ο παραδοσιακός φάκελος ασθενή περιέχει μια πληθώρα δεδομένων που, κατά κύριο λόγο, εισάγονται από γιατρούς και νοσηλευτές, αλλά και από άλλους επαγγελματίες υγείας ή διοικητικό προσωπικό. Εκτός από τις προσωπικές εκτιμήσεις των συγκεκριμένων χρηστών, στο φάκελο ασθενή εισάγονται τα αποτελέσματα των εργαστηριακών εξετάσεων, οι ακτινογραφίες, οι αξονικές τομογραφίες, τα υπερηχογραφήματα, τα ηλεκτροκαρδιογραφήματα, τα ηλεκτροεγκεφαλογραφήματα, τα αποτελέσματα βιοψιών και πλήθος άλλων πληροφοριών σχετικά με κάθε ασθενή. Αν εξαιρέσει κανείς κάποιες εξετάσεις, οι οποίες εμφανίζονται με τη μορφή διαγραμμάτων, και τις εικόνες, τα περισσότερα δεδομένα εμφανίζονται ως κείμενο ή αριθμοί. Τέλος, στα περισσότερα νοσοκομειακά ιδρύματα οι φάκελοι ασθενή είναι χειρόγραφοι, είτε εξ ολοκλήρου είτε στο μεγαλύτερο μέρος τους.

Ωστόσο, τα διαφαινόμενα οφέλη από τη διατήρηση των φακέλων σε ηλεκτρονική μορφή, μέσα από τη δημιουργία ισχυρών υπολογιστικών συστημάτων που υποστηρίζουν την αποθήκευση, διατήρηση και επεξεργασία των δεδομένων ασθενή, πιέζουν για τη μετάβαση από το χειρόγραφο φάκελο στον ηλεκτρονικό φάκελο ασθενή).

Σκοπός, λοιπόν, της εργασίας αυτής είναι η διερεύνηση της μετάβασης από τον ιατρικό φάκελο στον ηλεκτρονικό ιατρικό φάκελο και τα οφέλη που μπορεί αυτός να επιφέρει τόσο στην υγεία, όσο και στον ίδιο τον ασθενή.

Στο πρώτο κεφάλαιο της εργασίας γίνεται αναφορά στην έννοια της πληροφορίας και των δεδομένων αρχικά, ενώ στη συνέχεια διερευνά τις έννοιες των πληροφοριακών συστημάτων γενικά αλλά και των πληροφοριακών συστημάτων υγείας. Αναφορά γίνεται επίσης στην ηλεκτρονική υγεία (e-health).

Το δεύτερο κεφάλαιο επικεντρώνεται στον ηλεκτρονικό φάκελο υγείας. Μελετά τη δομή του, καθώς και τα συστήματα ηλεκτρονικού φακέλου υγείας που υπάρχουν. Επιπλέον, παρουσιάζονται οι χρήσεις του ηλεκτρονικού φακέλου, όπως και πλεονεκτήματα αλλά και τα μειονεκτήματα αυτού.

Τέλος, το τρίτο κεφάλαιο αναφέρεται στην ασφάλεια του ηλεκτρονικού φακέλου. Διερευνά την ιδιωτικότητα, την εμπιστευτικότητα και την ακεραιότητά του. Ενώ, στο τέλος παρουσιάζει το νομοθετικό και θεσμικό πλαίσιο στην Ελλάδα.

Κεφάλαιο 1

Νέες Τεχνολογίες και Υγεία

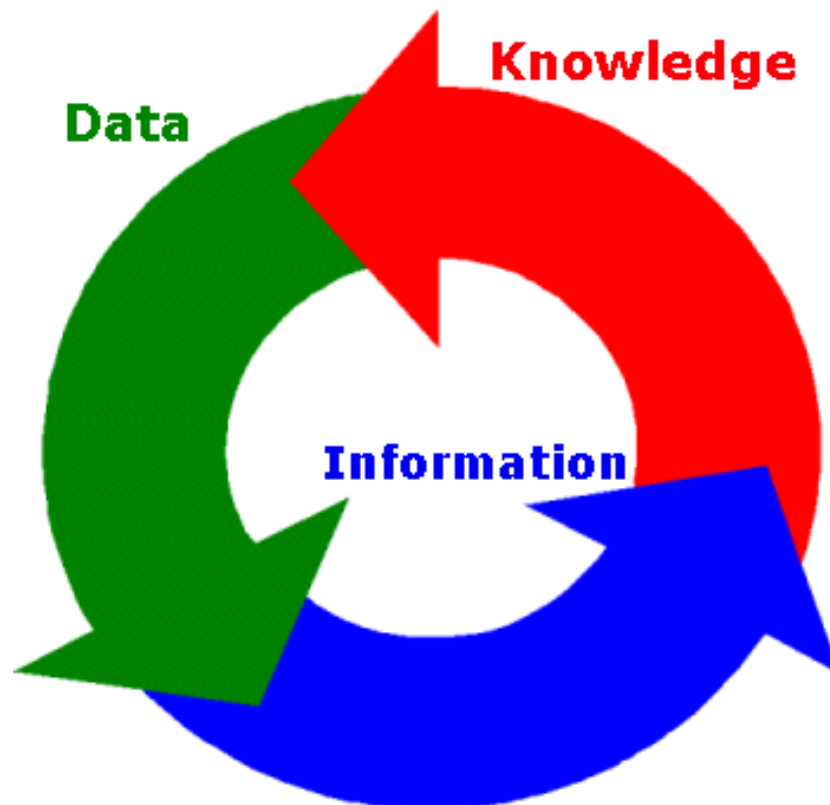
1.1 Η Έννοια της Πληροφορίας

Στην προσπάθεια να γίνει μια διάκριση ανάμεσα στα δεδομένα και στην πληροφορία, ένα παράδειγμα θα ήταν ότι, όταν αναφέρει κανείς τη λέξη «δέκα» προφανώς δε σημαίνει τίποτα, όμως το δεδομένο αυτό μπορεί να μετατραπεί σε σημαντική πληροφορία μόνο αν τεθεί σε γνωστά συμφραζόμενα. Δηλαδή, αν είχε γίνει η ερώτηση «ποιες ήταν οι πωλήσεις της εταιρείας φέτος», τότε με το «δέκα» θα είχε δοθεί μια πληροφορία παρά ένα δεδομένο, και μάλιστα αν ήταν ήδη γνωστό ότι οι πωλήσεις μετριοούνται σε χιλιάδες ευρώ.

Η πληροφορία, λοιπόν, αποτελεί μία προσαύξηση στη διαδικασία γνώσης. Συνεισφέρει στο γενικό πλαίσιο των εννοιών και των γεγονότων που είναι γνωστά. Η πληροφορία βασίζεται στα συμφραζόμενα και στη γενική γνώση του αποδέκτη. Για να ληφθεί μία πραγματικά σημαντική πληροφορία στο παραπάνω παράδειγμά, δεν θα έπρεπε απλώς να είναι γνωστό ότι το «δέκα» σημαίνει δέκα χιλιάδες ευρώ, αλλά θα έπρεπε επίσης να είναι γνωστές και τις πωλήσεις της εταιρείας φέτος. Αν το πληροφοριακό σύστημα δίνει τη δυνατότητα να εξηγηθεί η πτώση των πωλήσεων (π.χ. μειώθηκαν οι ενεργοί πελάτες και αυξήθηκε η τιμή πώλησης των προϊόντων), τότε η πληροφορία γίνεται γνώση (Κιουντούζης, 2009).

Τα δεδομένα είναι απλώς τα γεγονότα, το υλικό για τη λήψη πληροφοριών. Τα πληροφοριακά συστήματα χρησιμοποιούν τα δεδομένα που είναι αποθηκευμένα σε βάσεις δεδομένων για να παρέχουν τις απαραίτητες πληροφορίες. Η βάση δεδομένων είναι μία οργανωμένη συλλογή αλληλοσυσχετισμένων δομένων που αντανακλούν μία κύρια πτυχή των δραστηριοτήτων μίας εταιρείας.

Τα πληροφοριακά συστήματα παίρνουν δεδομένα από έναν οργανισμό (εσωτερικά δεδομένα) και το περιβάλλον του (εξωτερικά δεδομένα) και τα αποθηκεύουν για ένα χρονικά διάστημα. Όταν χρειαστούν κάποιες συγκεκριμένες πληροφορίες, επεξεργάζονται τα κατάλληλα δεδομένα και ο χρήστης λαμβάνει την πληροφορία που προκύπτει. Ανάλογα με το είδος του πληροφοριακού συστήματος, η απόδοση της πληροφορίας μπορεί να πάρει τη μορφή απάντησης σε ερώτηση βάσης δεδομένων, έκβασης απόφασης προτεινόμενης από ένα σύστημα υποστήριξης αποφάσεων, εξειδικευμένης συμβουλής από ένα έμπειρο σύστημα, αρχείου συναλλαγής ή αναφοράς. Είναι ξεκάθαρο ότι η αξία της πληροφορίας είναι πολύ μεγαλύτερη από αυτή των δεδομένων και βέβαια πολύ σημαντική όταν γίνεται γνώση (Turban, Volonino, 2012).



Εικ. 1.1 Από τα δεδομένα στη γνώση ¹

¹ Πηγή: <http://sc.readle.org.uk/images/datainfo.gif>

1.1.1 Πληροφορία στην Επιχείρηση

Η επιχείρηση είναι ένα ανοιχτό σύστημα, λόγω της συνεχούς αλληλεπίδρασης με το περιβάλλον της. Η επιχείρηση αλληλεπιδρά με το περιβάλλον της μέσω των συναλλαγών με τρίτους, ενώ παράλληλα η εσωτερική της λειτουργία βασίζεται στους μετασχηματισμούς των εισροών σε εκροές με τη βοήθεια των εσωτερικών διεργασιών. Βασικά η λειτουργία της επιχείρησης εκφράζεται με ένα συνεχή μετασχηματισμό υλικών και υλών σε χρήμα και αντίστροφα. Συνεπώς η πληροφορία είναι αποτέλεσμα των συνεχών διεργασιών μέσα στην επιχείρηση. Βασική προϋπόθεση για τη σωστή λειτουργία της επιχείρησης είναι η αξιοποίηση των δεδομένων και η παρακολούθηση των πληροφοριακών στοιχείων που προκύπτουν από τις διεργασίες. Παραδείγματος χάριν, η πώληση προϊόντων δημιουργεί το μετασχηματισμό τους σε χρήμα. Αυτή η διεργασία παράγει πληροφοριακά στοιχεία όπως το τιμολόγιο, το δελτίο αποστολής, τα δελτία παράδοσης και παραλαβής. Άρα η πληροφορία αποτελεί μέσο συγκέντρωσης και καταγραφής και επομένως και μέσο μελέτης της λειτουργίας της επιχείρησης. Η πληροφορία είναι ένα σημαντικό περιουσιακό στοιχείο για την επιχείρηση και με τη σωστή της διαχείριση μπορεί να συμβάλει σημαντικά στη μεγέθυνση της επιχείρησης. Συνεπώς, η πορεία εξέλιξης μιας επιχείρησης εξαρτάται σε μεγάλο βαθμό από την ποιότητα και την ποσότητα διαθέσιμων πληροφοριών, καθώς και από ορθή επεξεργασία τους για τη διαμόρφωση της απαιτούμενης πληροφόρησης (Παπαδάκη, 2007).

1.1.2 Γνώση στην Επιχείρηση

Η γνώση βασίζεται στις πληροφορίες και οι πληροφορίες στα δεδομένα. Τα δεδομένα είναι ακατέργαστα στοιχεία, τα οποία συλλέγονται από διάφορες πηγές εντός και εκτός της επιχείρησης και τα οποία περιγράφουν γεγονότα, πράγματα, έννοιες. Η πληροφορία είναι αποτέλεσμα διαλογής, επεξεργασίας ή/και σύνθεσης των δεδομένων.

Η γνώση αποτελεί τη συνολική εικόνα μέσω της οποίας παρέχεται ένα ολοκληρωμένο σύνολο πληροφοριών (π.χ. ο διευθυντής πωλήσεων μιας επιχείρησης έχει γνώση για την κίνηση των αποθεμάτων σε προϊόντα της επιχείρησης, όταν γνωρίζει τις ημερομηνίες εισαγωγής τους στις αποθήκες της επιχείρησης). Όταν το σύνολο αυτό των πληροφοριών είναι ακριβές και κατανέμεται σωστά στη διοικητική ιεραρχία της επιχείρησης ανάλογα με την ανάγκη

αξιοποίησης της πληροφορίας, τότε η γνώση είναι η καλύτερη δυνατή, με αποτέλεσμα να μειώνονται τα επίπεδα αβεβαιότητας, τα οποία εμφανίζονται σε κάθε επιχειρηματική απόφαση.

Η γνώση, σωστή ή λανθασμένη, μπορεί να επηρεάσει σημαντικά την πορεία μιας επιχείρησης. Αυτή μπορεί να χρησιμοποιηθεί ως ένα μέσο για την απόκτηση ανταγωνιστικού πλεονεκτήματος. Μια επιχείρηση που έχει πρόσβαση σε μοναδικές πληροφορίες μπορεί να κινηθεί επιχειρηματικά με σκοπό να βελτιώσει τη θέση της σε σχέση με τους ανταγωνιστές της. Η γνώση συνεπώς αποτελεί ένα σημαντικό άυλο πάγιο περιουσιακό στοιχείο και θα πρέπει κάθε επιχείρηση να δίνει μεγάλη βαρύτητα στη σωστή αξιοποίησή της διαφορετικά το κόστος της μη σωστής παροχής πληροφοριών και πληροφόρησης μπορεί να επιβαρύνει τη θέση της επιχείρησης μέσα στον κλάδο. Οι πόροι της επιχείρησης παραδοσιακά θεωρούνται η γη, τα κτίρια, το προσωπικό, τα χρήματα, τα υλικά και μηχανήματα. Αυτά είναι τα φυσικά πάγια που είναι δύσκολο να παραλειφθούν. Σήμερα η γνώση θεωρείται το ίδιο σημαντική όπως και τα υπόλοιπα πάγια στοιχεία της εταιρείας. Είναι γεγονός ότι το πραγματικό πλεονέκτημα στον ανταγωνισμό των επιχειρήσεων προέρχεται όχι μόνο από το υλικά, αλλά και από τα άυλα περιουσιακά στοιχεία. Αυτή η άποψη απορρέει από το γεγονός ότι όλοι οι πόροι μπορούν να αγοραστούν γρήγορα, αλλά η ανάπτυξη τεχνογνωσίας για τη συλλογή επιχειρηματικών πληροφοριών συνήθως διαρκεί χρόνια (Μπουραντάς, 2002).

Τα πλεονεκτήματα της γνώσης είναι εμφανή μόνο όταν η πληροφορία είναι διάχυτη μέσα στην επιχείρηση και επομένως δεν είναι σημαντικό να κατέχει μόνο κάποιος την πληροφορία. Όπως συμβαίνει και με τα άλλα πάγια στοιχεία η κατοχή τους δεν έχει τόσο μεγάλη σημασία, όσο η χρησιμοποίησή τους που δείχνει την χρησιμότητα της.

1.2 Η Αξία των Νέων Τεχνολογιών

Η σημερινή εποχή χαρακτηρίζεται ως η εποχή των συγκεχυμένων μέσων και σκοπών, είναι η εποχή της τεχνολογίας και του πολιτισμού. Καθημερινά ο άνθρωπος γίνεται δέκτης ενός τεράστιου αριθμού μηνυμάτων και αναγκάζεται πολλές φορές να κατευθύνει τη ζωή του ανάλογα με τα μηνύματα που λαμβάνει. Άρα η εποχή η ίδια υποδεικνύει τις συνθήκες ζωής του ανθρώπου και μέσω της πληροφόρησης δίνει στον άνθρωπο τα κατάλληλα εφόδια για να αντιμετωπίσει όλα τα προβλήματά του.

Με τον όρο πληροφόρηση εννοείται η μετάδοση γνώσεων, ιδεών και διαφόρων άλλων ερεθισμάτων. Γίνεται με διάφορα μέσα όπως με την τηλεόραση, το τηλέφωνο, τον τύπο, το διαδίκτυο. Παλιότερα, τα πράγματα ήταν πολύ δύσκολα, γιατί οι άνθρωποι είχαν να αντιμετωπίσουν πολλά εμπόδια, όπως το ότι δεν υπήρχαν τα σύγχρονα μέσα τα οποία κάνουν δυνατή την πληροφόρηση, επιπλέον οι μεγάλες αποστάσεις και η γεωγραφία του τόπου δεν επέτρεπαν τη διάδοση μηνυμάτων τόσο εύκολα όσο σήμερα (Κούτρας, 2005).

Αφήνοντας πίσω το παρελθόν και κοιτώντας στο παρόν θα δούμε ότι ο άνθρωπος με τον πολυμερέστατο νου κατάφερε να μικρύνει τις αποστάσεις να μικρύνει το χρόνο και τελικά να φέρει σε επικοινωνία όχι μόνο τα άτομα μιας κοινωνίας αλλά ολόκληρους τους λαούς. Μέσω της πληροφόρησης πάρθηκαν σπουδαίες αποφάσεις που καθόρισαν το μέλλον της ανθρωπότητας.

Όλα αυτά βέβαια έχουν πραγματοποιηθεί χάρη στην ανάπτυξη της τεχνολογίας και της επιστήμης, η οποία βοηθά στην πρόοδό τους. Εάν η τεχνολογία δεν παρουσίαζε ραγδαία ανάπτυξη, ο άνθρωπος θα είχε παραμείνει στάσιμος.

1.3 Η Έννοια των Πληροφοριακών Συστημάτων

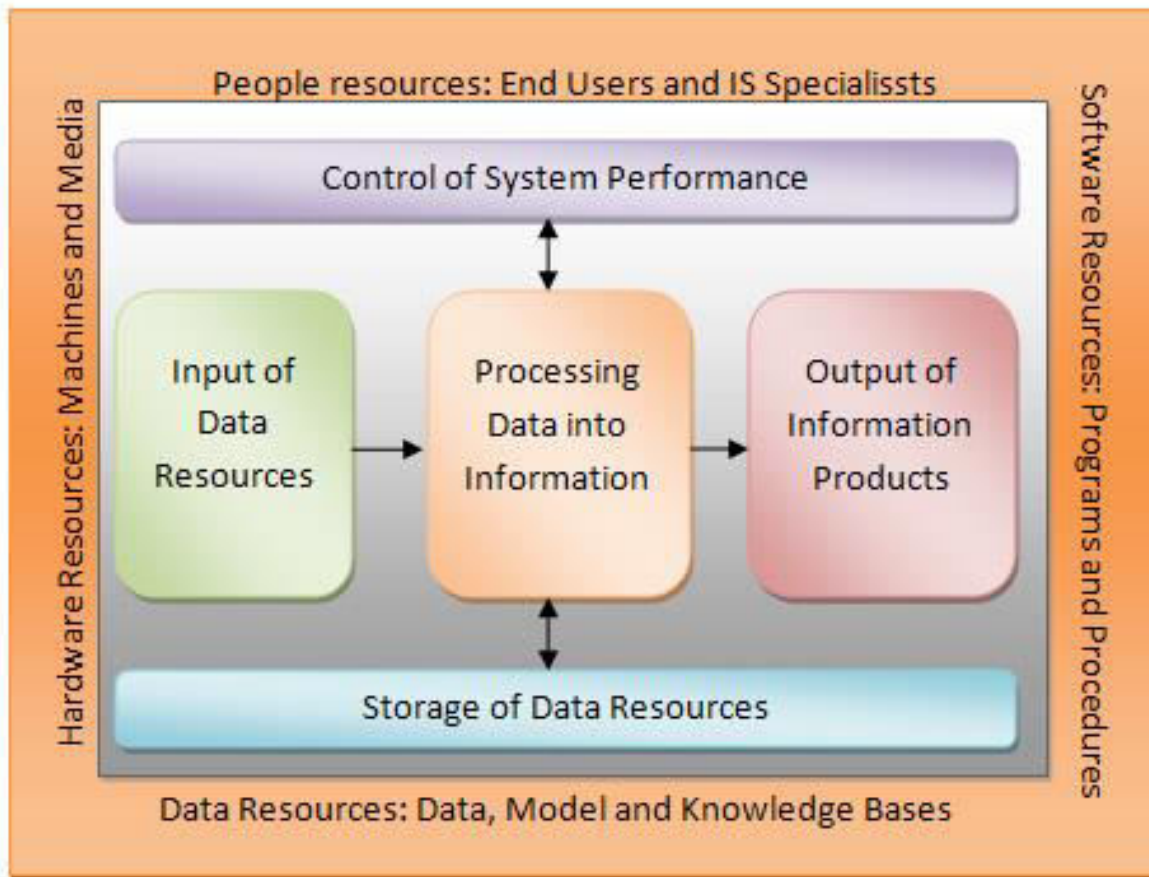
1.3.1 Ορισμός

Σύμφωνα με τους Laudon και Laudon (2009), «Ένα πληροφοριακό σύστημα μπορεί να οριστεί τεχνικά ως ένα σύνολο αλληλοσχετιζόμενων στοιχείων, τα οποία συλλέγουν (ή ανακτούν), επεξεργάζονται, αποθηκεύουν, και διανέμουν πληροφορίες που υποστηρίζουν τη λήψη αποφάσεων και τον έλεγχο σε έναν οργανισμό. Επιπλέον της υποστήριξης στη λήψη αποφάσεων, στο συντονισμό, και στον έλεγχο, τα συστήματα πληροφοριών μπορούν, επίσης, να βοηθούν τα στελέχη και το προσωπικό στην ανάλυση προβλημάτων, στην απεικόνιση σύνθετων θεμάτων, και στη δημιουργία νέων προϊόντων».

Σε ένα Πληροφοριακό Σύστημα, είτε είναι χειρόγραφο, είτε μηχανογραφικό, πραγματοποιούνται οι ακόλουθες διεργασίες:

- Συλλογή δεδομένων: Τα δεδομένα που μπορούν να είναι αριθμοί, ημερομηνίες, γεγονότα, συζητήσεις, διαδόσεις κ.λπ., συλλέγονται.
- Αποθήκευση δεδομένων: Τα δεδομένα μπορούν να αποθηκεύονται στο ανθρώπινο μυαλό, σε καρτελοθήκη, σε αρχείο ή βάση δεδομένων Η/Υ.

- Επεξεργασία δεδομένων: Είναι κυρίως ανάλυση, κωδικοποίηση, ταξινόμηση, αριθμητική επεξεργασία και σύνθεση των δεδομένων.
- Παρουσίαση της πληροφορίας: Γίνεται με την κατάλληλη μορφή που υπαγορεύει το μοντέλο του συστήματος.



Εικόνα 1.2 :Πληροφοριακά Συστήματα ²

1.3.2 Συστατικά Μέρη Πληροφοριακού Συστήματος

Το πληροφοριακό σύστημα μιας επιχείρησης είναι ένα σύστημα που αποτελείται από τους ανθρώπους, τις διαδικασίες και τον εξοπλισμό, μέσω των οποίων παράγονται, φυλάσσονται, διακινούνται, επεξεργάζονται, μετασχηματίζονται, αποθηκεύονται και διαχέονται

² Πηγή: <http://www.business-intelligence-secrets.com/wp-content/uploads/2011/04/Information-system.jpg>

οι πληροφορίες που είναι χρήσιμες για την επίτευξη των σκοπών της επιχείρησης. Μέσω του πληροφοριακού συστήματος, οι πληροφορίες ρέουν από το ένα άτομο ή το ένα τμήμα στο άλλο, με διάφορους τρόπους: εσωτερική αλληλογραφία, τηλέφωνα, έντυπες καταστάσεις από τον ηλεκτρονικό υπολογιστή, οθόνες τερματικών, κλπ. Το πληροφοριακό σύστημα εξυπηρετεί όλες τις οργανωτικές μονάδες της επιχείρησης, συνδέοντας τα διάφορα υποσυστήματα, έτσι ώστε να μπορούν να συνεργάζονται αποδοτικά προς τον κοινό σκοπό. Τα βασικά συστατικά μέρη ενός πληροφοριακού συστήματος είναι (Avison, Fitzgerald, 2006):

Άνθρωποι

Οι άνθρωποι είναι εκείνοι που παράγουν τις πληροφορίες και τις χρησιμοποιούν για να πάρουν αποφάσεις είτε σε καθημερινά ζητήματα ρουτίνας, είτε σε έκτακτα ή σημαντικά προβλήματα. Είναι ο σημαντικότερος παράγων κατά την επιλογή και υλοποίηση ενός πληροφοριακού συστήματος, αφού είναι ο χρήστης.

Διαδικασίες

Διαδικασία είναι μια σειρά από οδηγίες που καθορίζουν τον τρόπο με τον οποίο θα ενεργήσουν οι άνθρωποι σε συγκεκριμένες περιστάσεις. Οι διαδικασίες υποστηρίζουν τις ανθρώπινες δραστηριότητες, εξασφαλίζουν ότι ο κατάλληλος άνθρωπος θα πάρει την κατάλληλη πληροφορία στην κατάλληλη στιγμή και καθορίζουν τον τρόπο με τον οποίο θα μετασχηματιστούν οι πληροφορίες. Οι διαδικασίες μπορεί να είναι πάγιες ή έκτακτες, γραπτές ή προφορικές, επίσημες ή άτυπες. Είναι καθορισμένος τρόπος εκτέλεσης μιας δραστηριότητας ή διεργασίας του πληροφοριακού συστήματος.

Εξοπλισμός (Μέσα)

Είναι όλα τα μέσα που χρησιμοποιούνται για τη φύλαξη, διακίνηση και επεξεργασία των πληροφοριών.

Ένα Πληροφοριακό Σύστημα βασισμένο σε Η/Υ περιλαμβάνει (Behrouz, Firouz, 2010):

- Λογισμικό (Software), δηλαδή προγράμματα ηλεκτρονικών υπολογιστών, δομές δεδομένων και η σχετική τεκμηρίωση τους. Το λογισμικό υλοποιεί τη λογική της μεθοδολογίας της διαδικασίας ή του ελέγχου που απαιτείται, προς εξυπηρέτηση, άμεσα του χρήστη και έμμεσα ολόκληρου του παραγωγικού συστήματος. Παράγει με τον τρόπο αυτό πληροφορίες δηλαδή επεξεργασμένα δεδομένα σε ωφέλιμη μορφή για αυτόν που τα αποκτά.
- Υλικό (Hardware), δηλαδή επεξεργαστές σκληροί δίσκοι, οθόνες εκτυπωτές κλπ. Βάση Δεδομένων

Τα δεδομένα είναι η απαραίτητη πρώτη ύλη η οποία πρέπει να μετασχηματιστεί σε πληροφορία μέσα από το πληροφοριακό σύστημα. Είναι μια μεγάλη οργανωμένη συλλογή δεδομένων, η οποία σε ένα Πληροφοριακό Σύστημα βασισμένο σε ΗΥ, επεξεργάζεται με τη βοήθεια λογισμικού, το οποίο ονομάζεται Σύστημα Διαχείρισης Βάσεων Δεδομένων.

Τεκμηρίωση

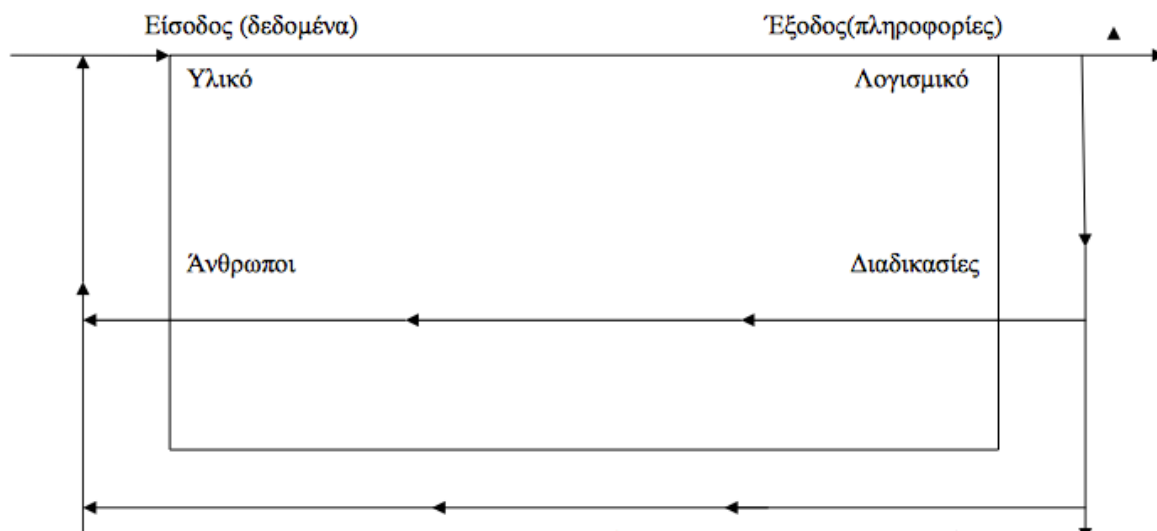
Εγχειρίδια, φόρμες και κάθε άλλου είδους επεξηγηματική γραπτή πληροφορία που καθορίζει τη χρήση και τη λειτουργία του συστήματος.

Μέχρι πριν από λίγα χρόνια, τα μέσα επηρέαζαν ελάχιστα τον τρόπο λειτουργίας ενός πληροφοριακού συστήματος. Στην εποχή μας όμως, οι καταλυτικές εξελίξεις στον τομέα των ηλεκτρονικών υπολογιστών και των τηλεπικοινωνιών έδωσαν στα μέσα ένα νέο σημαντικό ρόλο. Πολλές φορές συμβαίνει να δημιουργείται ένα νέο πληροφοριακό σύστημα ή μια επιχείρηση ή και ένας ολόκληρος επιχειρησιακός τομέας με αφορμή την εφεύρεση και διάθεση ενός καινούργιου επαναστατικού μέσου αποθήκευσης, διακίνησης ή επεξεργασίας πληροφοριών.

Όπως όλα τα συστήματα, έτσι και τα πληροφοριακά, έχουν εισροές (inputs), που μέσω κάποιας επεξεργασίας μετατρέπονται σε εκροές (outputs), λειτουργούν σε ένα δεδομένο περιβάλλον, ενώ υπάρχει και ένας μηχανισμός ανατροφοδότησης (feedback) για τον έλεγχο των αποτελεσμάτων, που συνήθως είναι μέτρηση-σύγκριση- διόρθωση.

Στα Πληροφοριακά Συστήματα οι έννοιες είσοδος, έξοδος, επεξεργασία και ανατροφοδότηση έχουν το εξής περιεχόμενο (Κιουντούζης, 2009):

- Είσοδος (Εισροές): είναι η συλλογή ή απόκτηση ακατέργαστων δεδομένων που προέρχονται είτε από το εσωτερικό της επιχείρησης, είτε από το εξωτερικό της περιβάλλον.
- Επεξεργασία: είναι η μετατροπή, ο χειρισμός και η ανάλυση των ακατέργαστων δεδομένων
- Έξοδος (Εκροές): είναι η διανομή και η διάχυση των επεξεργασμένων πληροφοριών στα άτομα ή στις δραστηριότητες.
- Ανατροφοδότηση: είναι ο μηχανισμός ελέγχου και αναθεώρησης του συστήματος για να είναι δυνατή η τροποποίηση και η βελτίωση του.



Εικόνα 1.3 :Συστατικά πληροφοριακού συστήματος³

1.4 Ηλεκτρονική Υγεία (e-Health)

Ο όρος "ηλεκτρονική υγεία" (e-Health) καλύπτει ένα ευρύ φάσμα εργαλείων βασισμένων στις τεχνολογίες πληροφοριών και επικοινωνιών που στοχεύουν στην καλύτερη πρόληψη, διάγνωση, θεραπεία, παρακολούθηση και διαχείριση της υγείας και του τρόπου ζωής (Καπόπουλος, Τσιμπουκέλης, 2010).

³ Πηγή: <http://nefeli.lib.teicrete.gr/browse/sdo/log/2012/PsomasDimitrios/attached-document-1349866039-752055-21139/Psomas2012.pdf>

Με την ηλεκτρονική υγεία γίνεται δυνατή η συνεργασία ανάμεσα στους φορείς που παρέχουν υγειονομικές υπηρεσίες και του ασθενείς, τα ιδρύματα μπορούν και ανταλλάσσουν δεδομένα μεταξύ τους, οι ασθενείς επικοινωνούν μεταξύ τους και με τους υπαλλήλους στον τομέα υγείας. Στην ηλεκτρονική υγεία περιλαμβάνονται επίσης δίκτυα πληροφοριών για την υγεία, υπηρεσίες τηλεϊατρικής, ηλεκτρονικά μητρώα καθώς και ατομικά ενδυτά και φορητά επικοινωνούντα συστήματα για την παρακολούθηση και στήριξη ασθενών.

Με τα εργαλεία ηλεκτρονικής υγείας μπορεί κανείς να πληροφορηθεί για θέματα υγείας τα οποία πολλές φορές είναι χρήσιμα για την ζωή του, αφού όλο και περισσότερο γίνεται μεγαλύτερη η διασυννοριακή κυκλοφορία ασθενών και πολιτών. Τα οφέλη της ηλεκτρονικής υγείας είναι σημαντικά στην κοινωνία, αφού με αυτή βελτιώνεται η πρόσβαση στην παρεχόμενη περίθαλψη και την ποιότητά της. Επίσης, βοηθάει να αναπτυχθούν περισσότερο τα συστήματα υγείας που είναι προσανατολισμένα στον πολίτη και κυρίως στην βιωσιμότητα και αποδοτικότητα του τομέα υγείας (Σαραντινού, 2013).

Η Ευρωπαϊκή Ένωση διευκολύνει και ρυθμίζει δράσεις ανάμεσα σε ενδιαφερόμενους φορείς και πολίτες με στόχο την διάδοση ορθών πρακτικών και την εξεύρεση καλύτερων λύσεων. Οι κυριότεροι στόχοι είναι να δημιουργηθεί ένα σύστημα ηλεκτρονικών μητρώων υγείας όπου θα μπορεί κανείς να ανταλλάσει πληροφορίες, η ανταλλαγή πληροφοριών ανάμεσα σε δίκτυα ανταλλαγής πληροφοριών για την υγεία, ώστε στην περίπτωση κινδύνου για την δημόσια υγεία να υπάρχει συντονισμός, η απευθείας παροχή υπηρεσιών με ειδική σύνδεση, η ηλεκτρονική συνταγογράφηση, η ανάπτυξη συστημάτων τηλεσυμβουλευτικής. Για την επιτυχία αυτού του εγχειρήματος θα πρέπει να ληφθούν υπόψη οι ανάγκες των ασθενών, των πολιτών και των εργαζομένων στον τομέα υγείας και συγχρόνως να εξασφαλισθεί η συμμετοχή στην υλοποίηση των στρατηγικών και των σχεδίων.

1.5 Πληροφοριακά Συστήματα υγείας

Η σημαντική πρόοδος που έχει σημειωθεί τα τελευταία χρόνια στο χώρο της Βιοϊατρικής τεχνολογίας έχει δώσει νέες κατευθύνσεις στην ιατρική έρευνα, με έντονη την παρουσία του ηλεκτρονικού υπολογιστή και άλλων ψηφιακών συστημάτων. Συγχρόνως έχει δημιουργήσει πολλές νέες ανάγκες σε όλους τους φορείς Υγείας και ιδιαίτερα στα κέντρα ιατρικής περίθαλψης. Σήμερα, περισσότερο από κάθε άλλη φορά, υπάρχει μεγάλη ανάγκη επικοινωνίας και

συνεργασίας των ιατρών με άλλους επιστήμονες, καθώς και σωστής πληροφόρησης των παραγόντων που επωμίζονται τις ευθύνες και παίρνουν καθημερινά αποφάσεις που έχουν άμεσες και μακροπρόθεσμες συνέπειες για την ανθρώπινη Υγεία. Η Πληροφορική, βασιζόμενη στην τεχνολογία των ηλεκτρονικών υπολογιστών και των τηλεπικοινωνιακών δικτύων, ασχολείται με την επεξεργασία, οργάνωση, αποθήκευση και ανάκτηση πληροφοριών.

Έτσι, είναι η επιστήμη που καλείται και σήμερα διεθνώς (Γιούπιου, 2011):

- Να εξασφαλίσει τη σωστή πληροφόρηση όλων των φορέων Υγείας με βάση αντικειμενικά στατιστικά δεδομένα.
- Να λύσει προβλήματα εσωτερικής οργάνωσης των μονάδων Υγείας, επικοινωνίας μεταξύ διαφόρων τμημάτων των μονάδων Υγείας και συλλογής στατιστικών και άλλων στοιχείων που είναι αναγκαία για την εύκολη και αντικειμενική προσαρμογή κάθε κέντρου ιατρικής περίθαλψης σε ένα νέο Σύστημα Υγείας.
- Να διευκολύνει την επικοινωνία και συνεργασία γιατρών και άλλων επιστημόνων στην βασική και κλινική έρευνα.
- Να συντελέσει στην ολοκληρωμένη αντιμετώπιση του προβλήματος ανάλυσης και κατανόησης του πλήθους πληροφοριών άλλοτε συμπληρωματικών και άλλοτε αντικρουόμενων, που παράγονται από τα σύγχρονα ιατρικά όργανα σε μορφή βιολογικών σημάτων, εικόνων και εργαστηριακών αποτελεσμάτων μέσα στο γενικότερο πλαίσιο των ιατρικών γνώσεων.

Παρατηρείται σήμερα στην ιατρική, αυξημένη χρήση οργάνων των οποίων η λειτουργία ελέγχεται μέσω ηλεκτρονικού υπολογιστή και τα οποία παράγουν πληροφορίες που είναι ήδη σε ψηφιακή μορφή, δηλαδή μορφή που προσφέρεται για πρόσθετη επεξεργασία από ηλεκτρονικό υπολογιστή. Σαν παράδειγμα αναφέρει κανείς το χώρο της διαγνωστικής εικονογραφίας όπου ήδη ο ηλεκτρονικός υπολογιστής και τα ψηφιακά συστήματα εν γένει χρησιμοποιούνται ολοένα και περισσότερο στην σύνθεση και επεξεργασία όλων των διαγνωστικών εικόνων, στην καταχώρηση τους σε ηλεκτρονικά αρχεία και στην κωδικοποίηση και μετάδοση τους από μια ιατρική μονάδα σε άλλη. Είναι γνωστό ότι υπάρχουν έμπειρα συστήματα, τα οποία σε διαλογική συνεργασία με τον ειδικό ιατρό, χρησιμοποιούν κανόνες λογικής και αντλούν υλικό από δομημένες βάσεις δεδομένων (ιατρικών γνώσεων και μεθοδολογιών καθώς και διεθνώς αποδεκτής βιβλιογραφίας) για να κάνουν κριτική αξιολόγηση διαφόρων ιατρικών αποφάσεων ή και να δώσουν συγκεκριμένη διάγνωση.

Αποτέλεσμα της αυξημένης χρήσης νέων μεθόδων και οργάνων στη σύγχρονη ιατρική είναι να δίνεται σήμερα μεγάλη έμφαση στην εξειδίκευση ενώ παράλληλα γίνεται πιο έντονη η ανάγκη για μια περισσότερο συντονισμένη διαγνωστική επεξεργασία. Εκτός από τις σοβαρές συνέπειες που μπορεί να έχει η έλλειψη τέτοιου συντονισμού για τον ίδιο τον ασθενή, αυξάνει και το συνολικό κόστος ιατρικής περίθαλψης λόγω του μεγάλου αριθμού των περιπτώσεων εξετάσεων στις οποίες υποβάλλονται οι ασθενείς καθώς και της μεγαλύτερης παραμονής τους μέσα στο νοσοκομείο.

Η Πληροφορική σαν επιστήμη και τα συστήματα πληροφορικής γενικότερα μπορούν και πρέπει να παίξουν σημαντικό ρόλο στην προσπάθεια επίλυσης αυτών των προβλημάτων έτσι ώστε να μπορέσει η Ιατρική να ανταποκριθεί στις νέες ανάγκες και να προσαρμοστεί στις νέες κατευθύνσεις που έχουν δοθεί στην βασική και κλινική έρευνα (Τσαλουκίδης, Παπαγεωργίου, 2008).

Είναι σήμερα επιτακτικό κατά τη διάρκεια σχεδιασμού και μελέτης όχι μόνο του υπολογιστικού δυναμικού, αλλά και του γενικότερου εργαστηριακού, να εξετάζεται στις μονάδες Υγείας η τοποθέτηση ενός τοπικού δικτύου επικοινωνίας δεδομένων με πρόσβαση στο διαδίκτυο. Επίσης, είναι επιτακτική η δυνατότητα άντλησης κάθε είδους διοικητικών, φαρμακευτικών και άλλων πληροφοριών που αφορούν την αποδοτικότερη λειτουργία του συστήματος παροχής υπηρεσιών Υγείας.

1.5.1 Συστήματα Υγείας και Πληροφορική

Η διατήρηση και η βελτίωση της υγείας της ανθρώπινης κοινότητας απαιτεί - μεταξύ άλλων - την οργάνωση και λειτουργία ενός μεγάλου κοινωνικού συστήματος, το οποίο καλείται με το γενικό όρο Σύστημα Υγείας, στα πλαίσια του οποίου πραγματοποιείται η άσκηση της ιατρικής.

Η παραγωγή και η διανομή των φροντίδων υγείας βασίζεται στα δομημένα υποσύνολα του Συστήματος Υγείας, τις μονάδες παραγωγής υπηρεσιών υγείας (νοσοκομεία, κέντρα υγείας κ.α), οι οποίες αποτελούν παραγωγικές δομές μεγάλης έντασης και υψηλού καταμερισμού της εργασίας. Με αυτή την έννοια, η παραγωγική διαδικασία στις μονάδες υγείας προϋποθέτει την

οργάνωση και λειτουργία ενός συστήματος ροής και επεξεργασίας των πληροφοριών. Η αξία της πληροφορίας στην ιατρική περίθαλψη ανέρχεται εκθετικά. Ο τελικός στόχος της Πληροφορικής στο επίπεδο αυτό είναι η βελτίωση της περίθαλψης - και της υγείας - του πληθυσμού δια μέσου της αξιολόγησης των επιδημιολογικών δεδομένων (πρωτοβάθμια περίθαλψη, πρόληψη) και της βελτιωμένης αποτελεσματικότητας των διαφόρων υπηρεσιακών βαθμίδων του συστήματος υγείας (κέντρα υγείας, νοσοκομεία, επείγουσα περίθαλψη κλπ.) (Φαρατζιάν, 2007).

Με τον όρο Πληροφορική Υγείας, γενικά νοείται η επιστήμη και η τεχνολογία της επεξεργασίας πληροφοριών στον τομέα της υγείας (διοίκηση και διαχείριση νοσοκομείων και κέντρων υγείας, σχεδιασμός, προγραμματισμός, έλεγχος και αξιολόγηση συστημάτων υγείας κ.α.). Οι εφαρμογές της Πληροφορικής Υγείας αποσκοπούν στην εισαγωγή πληροφοριακών μεθόδων και συστημάτων στη διοίκηση, το σχεδιασμό και την αξιολόγηση των μονάδων-οργανισμών παραγωγής φροντίδων υγείας και συγκεκριμένα (Καρύδη, 2010):

- Στη διοίκηση-διαχείριση των μονάδων υγείας (π.χ. νοσοκομείων), τα πληροφοριακά συστήματα αναπτύσσονται στις διοικητικές και οικονομικές υπηρεσίες, στη διαχείριση των ανθρώπινων υλικών και οικονομικών πόρων, σε διαδικασίες ανάλυσης και ελέγχου κλπ.
- Στο σχεδιασμό των συστημάτων υγείας η πληροφορική χρησιμοποιείται στην εφαρμογή τεχνικών στατιστικής ανάλυσης, επιχειρησιακής έρευνας και προϋπολογιστικών τεχνικών στην προσπάθεια να υπολογιστεί το βάρος των διαφόρων παραμέτρων και να διευκολυνθεί η διαδικασία αποφάσεων και η ιεράρχηση προτεραιοτήτων.
- Στην αξιολόγηση και τον έλεγχο των συστημάτων υγείας η πληροφορική εφαρμόζεται στην εκτίμηση των αποτελεσμάτων του υγειονομικού τομέα (διαγνωστικές και θεραπευτικές διαδικασίες, δείκτες υγείας κ.α.) και στην παρακολούθηση της διοικητικής και οικονομικής λειτουργίας (νοσοκομειακή λογιστική, δαπάνες περίθαλψης κ.α.).



Εικόνα 1.4: Υποσύνολα Συστήματος Υγείας

1.5.2 Ιατρικά Πληροφοριακά Συστήματα

Ένα Ιατρικό Πληροφοριακό Σύστημα (ΙΠΣ) είναι ένα σύνολο υλικού (hardware), λογικού (software) και ανθρώπινου δυναμικού (liveware). Στην «καρδιά» του Ιατρικού Πληροφοριακού Συστήματος υπάρχει μία Βάση Δεδομένων με όλα τα απαραίτητα δεδομένα για την αποδοτική λειτουργία και διοίκηση ενός Νοσοκομείου, Κέντρου Υγείας, Γηροκομείου κλπ. Οι χρήστες του συστήματος έχουν πρόσβαση στη βάση δεδομένων για την αναζήτηση και τροποποίηση των στοιχείων της Βάσης Δεδομένων (Καρύδη, 2010).

Η βασική διαφορά των συστημάτων αυτών από τα άλλα Πληροφοριακά Συστήματα είναι ότι χειρίζονται ανθρώπους, γεγονός που απαιτεί από το σύστημα να παρέχει αξιοπιστία, ασφάλεια και ευελιξία. Η ταχύτητα και η ακρίβεια είναι δύο αντικειμενικοί στόχοι ενός Ιατρικού Πληροφοριακού Συστήματος. Επίσης στόχο έχει να δώσει περισσότερο χρόνο στους λειτουργούς των μονάδων υγείας (ιατρούς, νοσηλευτικό προσωπικό κλπ.), ώστε να παρέχουν καλλίτερες υπηρεσίες στους ασθενείς.

1.5.3 Πληροφορική και Υγεία

Η μετεξέλιξη της περίθαλψης από την Νοσο-Ιατροκεντρική στην πολύ ευρύτερη Υγειοκεντρική, μεταβάλλει τον ρόλο και τη σημασία της Πληροφορικής από υποστηρικτικό σε πρωτεύοντα, ιδίως με την αναπόφευκτη διασύνδεση Υγείας - Ασφάλισης - Περίθαλψης. Τα αναγκαία Δίκτυα Συστημάτων Υγείας, όπου η φροντίδα για την ασθένεια μετατρέπεται σε φροντίδα για την Υγεία απαιτούν για να υπάρχουν, Ενσωματωμένα Δίκτυα Πληροφορικής - ΕΔΠ (Integrated Health Information Systems). Με αυτά, η πληροφορία διατίθεται ευκολότερα, ταχύτερα και αποτελεσματικότερα αυξάνοντας την ποιότητα παροχής υπηρεσιών, καταργώντας λάθη ή γραφειοκρατία και ελαττώνοντας σημαντικά το κόστος.

Τα παραδείγματα από τις ΗΠΑ και την ΕΕ, χωρίς να αποτελούν υπόδειγμα κοινωνικής πολιτικής με τα πολλά και ποικίλα οικονομικά προβλήματα που αντιμετωπίζουν, αλλά με την εμφανώς καλύτερη οργάνωση των Συστημάτων Υγείας τους, αποδεικνύουν συλλογικά την παραπάνω αλήθεια και επιβεβαιώνουν στη πράξη το δόγμα ότι, οποιαδήποτε βελτίωση είναι δυνατή και εφικτή μόνο με ΕΔΠ. Η βασική αρχή της υγειοκεντρικής στροφής μετέτρεψε τον ασθενή στο άτομο-πρόσωπο με τις συγκεκριμένες ανάγκες αλλά και απαιτήσεις και δικαιώματα. Συγχρόνως, ο καθορισμός της αναγκαίας δομικής μονάδας συναλλαγής δοτών-δεκτών Υγείας, κατάργησε την ανεπαρκή ονομασία περιστατικό (encounter) και της έδωσε συγκροτημένο χαρακτηρισμό, με τον όρο, κάλυψη ζωής (covered life).

Κεφάλαιο 2

Ηλεκτρονικός Φάκελος

2.1 Η Έννοια του Ηλεκτρονικού Φακέλου Υγείας

Τα τελευταία χρόνια έχει πολλαπλασιαστεί ο αριθμός των πληροφοριών που είναι απαραίτητος για την φροντίδα ενός ασθενούς, φαινόμενο που οφείλεται στα πολλά αποτελέσματα παρακλινικών και εργαστηριακών εξετάσεων που πρέπει να καταχωρηθούν και να επεξεργαστούν. Επίσης, επειδή αυξάνεται η πολυπλοκότητα στην παροχή υγείας, συνεχώς αυξάνονται και τα διαχειριστικά καθήκοντα των γιατρών (Χουλιάρας, 2006).

Αποτέλεσμα της αύξησης των διαχειριστικών καθηκόντων είναι να μην είναι εύχρηστη, στην εποχή μας, η διαχείριση των υπηρεσιών μέσω της καταγραφής σε χαρτί και της καταχώρησης σε φακέλους, των εξετάσεων κάθε ασθενή, συνοδευόμενος με τις απαραίτητες εξετάσεις για κάθε περίπτωση. Οι νέες τεχνολογίες δίνουν την δυνατότητα να γίνει πιο εύκολη και αποτελεσματική η διαχείριση των υπηρεσιών αυτών, αφού παρέχει την δυνατότητα με την χρήση των υπολογιστών να αντικατασταθούν οι κλασικοί φακέλοι των ασθενών με Ηλεκτρονικούς Φακέλους Υγείας.

Στον Ηλεκτρονικό Φάκελο Υγείας καταγράφονται όλες οι ιατρικές εξετάσεις και πληροφορίες κάθε ασθενή, και παρέχει την δυνατότητα, στους παρόχους υπηρεσιών υγείας, πρόσβασης σε αυτόν, οποιαδήποτε στιγμή είναι απαραίτητο. Αποτελεί δηλαδή την βάση παροχής πληροφοριών για την θεραπευτική αντιμετώπιση και διάγνωση ασθένειας ενός ατόμου, αλλά παρέχει και πληροφορίες σε ερευνητές για επιδημιολογικές έρευνες. Επίσης παρέχει και πληροφορίες οικονομικής, στατιστικής και διοικητικής φύσεως για κάθε ασθενή, αλλά μπορεί κανείς να ενημερωθεί και για την ποιότητα της ιατροφαρμακευτικής περίθαλψης (Καλιμάνη, 2013).

Συμπεραίνει κανείς ότι ο ρόλος του Ηλεκτρονικού φακέλου είναι διπλός. Από την μία μεριά παρέχει ροή πληροφοριών στον κλινικό γιατρό και από την άλλη τον βοηθάει να συντάξει

ένα ολοκληρωμένο αρχείο για κάθε ασθενή ώστε να είναι σε θέση να αντιμετωπίσει έμμεσα ή άμεσα οποιαδήποτε ιατρική δραστηριότητα.

Λόγω της καταχώρηση των ιατρικών φακέλων σε ηλεκτρονικούς υπολογιστές, η αποθήκευση και ανάκληση νέων δεδομένων γίνεται γρήγορα, καθώς και η άμεση μεταφορά, και επεξεργασία τους σε οποιαδήποτε απόσταση. Παρατηρείται επομένως ότι το σύστημα καταγραφής δεδομένων για κάθε ασθενή, γίνεται πιο αποτελεσματικό αλλά και παρέχει την δυνατότητα να εμπλουτίζεται συνεχώς και με μεγάλη ευκολία (Αγγελόπουλος, 2012).

Ο φάκελος του κάθε ασθενούς συνοδεύεται πάντα με τις απαραίτητες εργαστηριακές εξετάσεις όπως ακριβώς έχουν επεξεργαστεί στο εργαστήριο. Τέτοιες εξετάσεις είναι οι βιοχημικές, το ηλεκτροκαρδιογράφημα, οι ακτινολογικές εξετάσεις κ.α. Είναι επομένως φυσικό να γίνεται ογκώδης ο φάκελος, με μεγάλη πιθανότητα κατά την μεταφορά του να παραπέσουν κάποια δεδομένα, ενώ δεν είναι άμεση η συσχέτιση με παλαιότερες εξετάσεις.

Στον Ηλεκτρονικό Φάκελο Υγείας γίνεται ενσωμάτωση όλων των δεδομένων που αφορούν τον ασθενή, χωρίς απαραίτητα να παίζει σπουδαίο ρόλο η μορφή τους. Στο κείμενο όπου καταγράφεται το ιστορικό, συνάπτονται και όλες οι εξετάσεις που έχουν προηγηθεί, βιοχημικές ή εργαστηριακές, και έτσι η ιατρική εικόνα γίνεται ολοκληρωμένη. Το περιεχόμενο του Ηλεκτρονικού Φακέλου Υγείας παρουσιάζει διαφορές ως προς τις πληροφορίες που απαιτούνται και το διάστημα που πρέπει να διατηρηθούν, τα δικαιώματα πρόσβασης, στον σκοπό, το πλήθος των πληροφοριών που πρόκειται να καταχωρηθούν, και το κόστος που θα χρειαστεί.

Τα δεδομένα που απεικονίζονται σε ένα Ηλεκτρονικό Φάκελο Υγείας ενός ασθενούς είναι (Μαγκλογιάννης, 2013):

- Κλινική εξέταση, εργαστηριακές εξετάσεις και ιστορικό με την μορφή κειμένου.
- Απεικονιστικές εξετάσεις όπως οι τομογραφίες και οι μαγνητικές εξετάσεις με την μορφή στατικών εικόνων (X-rays, CTs, MRIs,etc.).
- Ηλεκτροκαρδιογραφήματα με την μορφή βιο-σημάτων .
- Ενδοσκοπικές εξετάσεις
- Ηχοκαρδιογραφήματα σε μορφή ήχου
- Δημογραφικά στοιχεία του ασθενή

- Διαχειριστικά και οικονομικά στοιχεία ιατρικών πράξεων
- Παραπεμπτικά - Γνωματεύσεις

Στο σημείο αυτό αξίζει να αναφέρουμε ότι αναλύοντας τα παραπάνω δεδομένα είναι εμφανές ότι ένας πλήρης ηλεκτρονικός φάκελος υγείας αποτελεί μια οντότητα, η οποία αποτελείται από στοιχεία κειμένου, εικόνων, ήχων κλπ. Η κωδικοποίηση των στοιχείων αυτών αποτελεί ακόμα στοιχείο έρευνας καθώς προκύπτουν διαρκώς νέες τεχνολογίες διαχείρισης πληροφοριών.

Τα παραπάνω προϋποθέτουν την θέσπιση και εφαρμογή κωδικών και προτύπων, τα οποία θα καθορίζουν τον τρόπο συλλογής και παρουσίασης των δεδομένων από διαφορετικά πληροφοριακά συστήματα. Τα πρότυπα αυτά αναφέρονται στον τρόπο με τον οποίο πρέπει να γίνεται η μεταφορά πληροφορίας από ένα σύστημα σε κάποιο άλλο, αλλά και στο είδος της πληροφορίας που μπορεί να μεταφέρεται.

Ένα από τα σημαντικότερα διεθνή standards που έχουν αναπτυχθεί για την επικοινωνία μεταξύ Πληροφοριακών Συστημάτων ή/και ιατρικών μηχανημάτων είναι το πρωτόκολλο HL7 – Health Level 7, το οποίο είναι σήμερα το πλέον ευρέως χρησιμοποιημένο πρότυπο ανταλλαγής πληροφοριών μέσω ηλεκτρονικών μηνυμάτων στο χώρο της υγείας.

Οι κυριότερες ιδιότητες που πρέπει να έχει ένα λειτουργικό σύστημα Ηλεκτρονικού Φακέλου Υγείας είναι:

- Γρήγορη πρόσβαση σε αυτόν από τα εξουσιοδοτημένα άτομα.
- Ευελιξία και ευχρηστία για κάθε διαφορετική ομάδα χρειάζεται πληροφορίες.
- Διασφάλιση ότι η πρόσβαση θα γίνεται έγκαιρα
- Παροχή πληροφοριών από εξωτερικές βάσεις και σύνδεση με αυτές.
- Πρόσβαση μόνο από εξουσιοδοτημένα άτομα.
- Ελεγχιμότητα: Έλεγχοι σε κάθε είδος πρόσβασης και αλληλεπίδρασης σε συνάρτηση με τα αρχεία.
- Συντηρησιμότητα
- Εικοσιτετράωρη διαθεσιμότητα και γρήγορη απόκριση
- Λειτουργικό περιβάλλον αλληλεπίδρασης με τους χρήστες

2.2 Δομή Ηλεκτρονικού Φακέλου Υγείας

Ο φάκελος είναι ένα πρόγραμμα διαχείρισης βάσεων δεδομένων. Το ιστορικό του ασθενούς θα πρέπει να καταχωρείται στον Ηλεκτρονικό Φάκελο Υγείας, κατά τέτοιο τρόπο, ώστε η συσχέτιση μεταξύ των δεδομένων να είναι εύκολη και να διατηρηθούν (Χαντάκης, 2006).

2.2.1 Στοιχειώδης Πληροφορία (Item)

Στοιχειώδης ελάχιστη πληροφορία είναι η πληροφορία που από μόνης δίνει νόημα και προσδιορίζεται από το περιεχόμενό της. Παράδειγμα η πληροφορία «καρδιά» προσδιορίζει το όργανο της καρδιάς και η ιδιότητα «πίεση» αναφέρεται σε μία παθολογικής κατάστασης της καρδιάς. Η πληροφορία «πίεση» από μόνη της δεν αναφέρεται σε κάτι συγκεκριμένο και επομένως δεν χαρακτηρίζεται σαν στοιχειώδης πληροφορία (Δεσκέρε, Τσώλου, 2008). Με τις στοιχειώδεις πληροφορίες παρέχεται η δομή για την καταγραφή των τιμών των προς καταχώρηση στοιχείων (αριθμοί, τμήματα κειμένου, εικόνες, ήχοι, κλπ). Οι στοιχειώδεις πληροφορίες οργανώνονται σε υψηλότερες δομές, οι οποίες φέρουν περισσότερες πληροφορίες. Οι ομάδες στοιχειωδών πληροφοριών παρέχουν τη δυνατότητα για την αλλαγή του σκοπού των δεδομένων (φάρμακα : τρέχουσα αγωγή ή απλός κατάλογος για το φαρμακείο). Αποτελούν σύνολο στοιχειωδών πληροφοριών (μια ή περισσότερες) ή και υποομάδες στοιχειωδών πληροφοριών.

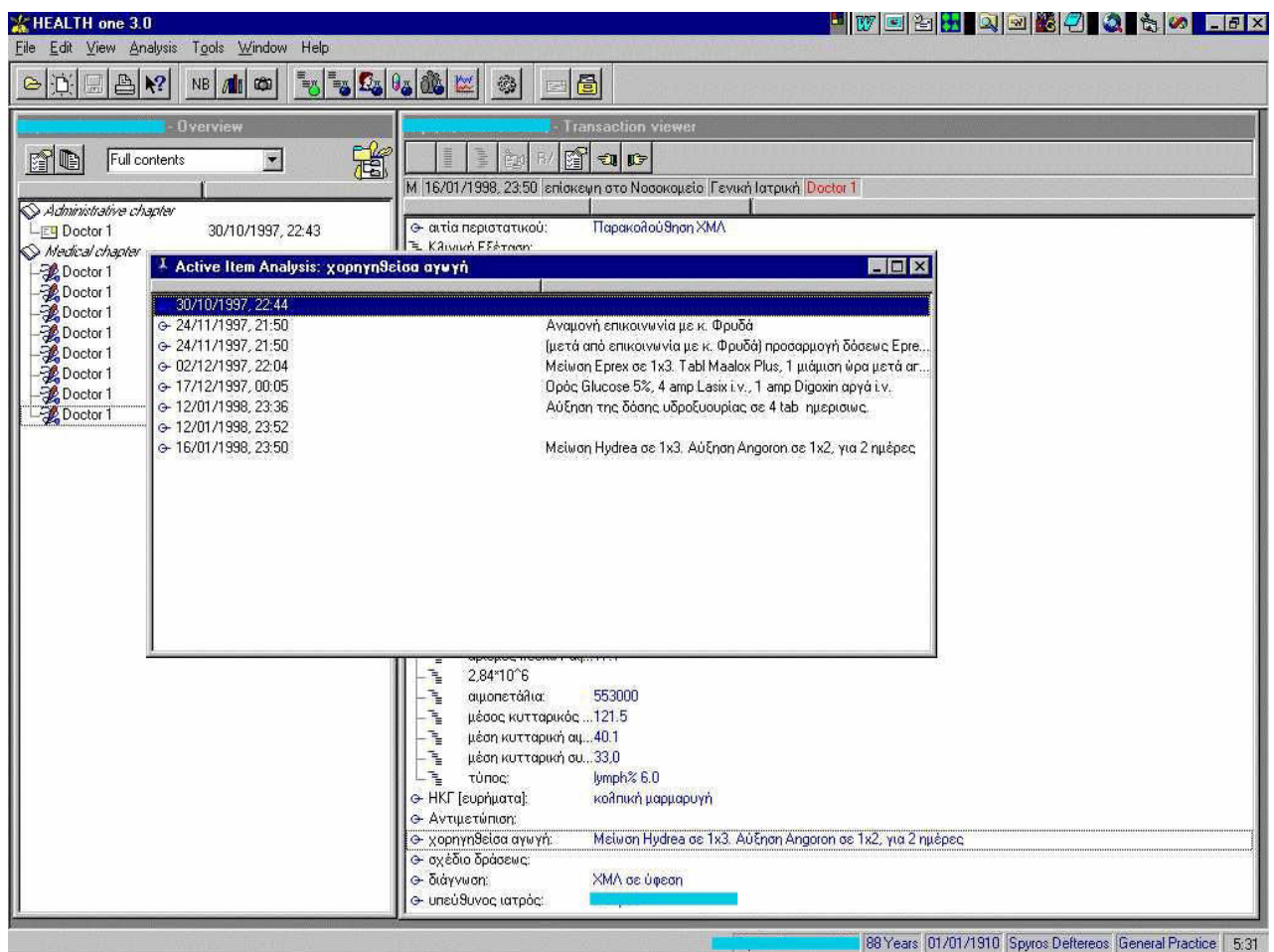
Έστω ότι ο λόγος επίσκεψης ήταν ανησυχία και πόνος στο επιγάστριο για 4 ημέρες, εμετός δύο φορές πριν 4 ημέρες. Οι πληροφορίες οργανώνονται ως εξής:[8]

- Ομάδα : πόνος
- Όνομα στοιχειώδους πληροφορίας : τόπος, τιμή : επιγάστριο
- Όνομα στοιχειώδους πληροφορίας : διάρκεια, τιμή : 4 (μονάδες : ημέρες)
- Όνομα στοιχειώδους πληροφορίας : σχόλιο, τιμή : ανησυχία

2.2.2 Επαφή (Contact), Επεισόδιο (Episode)

Στην επαφή (Contact), οργανώνονται οι πληροφορίες που είναι χρήσιμες για να περιγραφεί το ιατρικό ιστορικό ενός ασθενούς. Στην επαφή αυτή περιγράφονται τα δεδομένα που καταχωρούνται από μια επίσκεψη στον ιατρό ενός ασθενούς (Λούσα, 2010). Είναι οι πληροφορίες, οι οποίες καταγράφονται σχετικά με ένα ασθενή από ένα συγγραφέα/επαγγελματία υγείας, σε μιά μονάδα, κάποια χρονική στιγμή (καταγραφή των αποτελεσμάτων μιας εξέτασης, δημιουργία μιας έκθεσης σχετικά με το πρόβλημα του ασθενούς, ενσωμάτωση διαγνωστικών αποτελεσμάτων).

Επεισόδιο ονομάζεται μια σειρά επαφών όπου επισημαίνεται το ίδιο πρόβλημα σε ένα ασθενή. Στην περίπτωση αυτή ο φάκελος περιγράφει την πορεία της υγείας ενός ατόμου.



Εικόνα 2.1 :Αρχείο ασθενούς⁴

⁴ Πηγή: http://www.ebusiness-lab.gr/files/dmdocuments/Ptyxiakes/PDFs/deskere_ygeia.pdf

2.2.3 Ιατρικές, Διαχειριστικές Πληροφορίες (Medical, Administrative Information)

Το ιατρικό τμήμα του φακέλου ενός ασθενή περιγράφει το σύνολο των επισκέψεών του, καθώς και τις βασικές παραμέτρους του, πχ. την ομάδα αίματος, το κληρονομικό ιστορικό κ.α. (Χουλιάρας, 2006).

Εκτός από το ιατρικό τμήμα, στον φάκελο υπάρχει και το διαχειριστικό τμήμα όπου αναγράφονται πληροφορίες όπως του ασφαλιστικού τομέα στον οποίο ανήκει, το ονοματεπώνυμό του, η διεύθυνσή του κ.α.

Ο φάκελος με την αναγραφή των παραπάνω στοιχείων βοηθάει ώστε οι πληροφορίες να αποθηκεύονται και να μεταφέρονται γρήγορα. Η καταχώρηση του αριθμού των επαφών και των επεισοδίων, η απόδοση των κατάλληλων χαρακτηριστικών, και οι λοιπές πληροφορίες για τον ασθενή βοηθούν στην στοχευμένη αναπαράσταση της γνώσης του ασθενούς. Οι πληροφορίες που έχουν αποθηκευτεί με σωστό τρόπο, μπορούν αργότερα να διαβαστούν, να ανακληθούν και να επεξεργαστούν χωρίς οι πρώτες πληροφορίες να υποστούν αλλοίωση (Τσάκωνα, 2009).

ΙΑΤΡΙΚΟ ΙΣΤΟΡΙΚΟ ΣΥΓΓΕΝΩΝ ΑΣΘΕΝΟΥΣ 15/4/2006 11:36:10 πμ

Επώνυμο: ΔΟΚΙΜΗ Όνομα: ΔΟΚΙΜΗ Πατρώνυμο: ΔΟΚΙΜΗ

A.M.: 47114000000 Έτος Γένν.: 01/01/2006

Όνομ/μο συγγενούς: Είδος Σχέσης: Αριθμός Μητρώου:

ΔΙΑΛΕΞΤΕ ΜΟΝΟ ΟΣΑ ΕΧΟΥΝ ΣΧΕΣΗ

Εν Ζωή Ηλικία θανάτου: 0 Αν όχι, από θανάτου:

Καρκίνος Αν ΝΑΙ γράψτε το είδη του καρκίνου (π.χ. Ορθό, στήθος, προστάτης, δέρμα κλπ)

ΚΑΡΔΙΟΑΝΓΕΙΩΣΤΙΚΟ ΣΥΣΤΗΜΑ	ΓΑΣΤΡΟΕΠΙΠΕΡΟΛΟΓΙΚΟ ΣΥΣΤΗΜΑ	ΝΕΥΡΟΛΟΓΙΚΟ ΣΥΣΤΗΜΑ	ΆΛΛΑ ΟΡΓΑΝΑ/ΣΥΣΤΗΜΑΤΑ
<input type="checkbox"/> Στεφανιαία Νόσος	<input type="checkbox"/> ΓΟΠ	<input type="checkbox"/> Εγκεφαλικά	<input type="checkbox"/> Κίρρωση του ήπατος
<input type="checkbox"/> Υπέρταση	<input type="checkbox"/> Πεπτικά έλκη	<input type="checkbox"/> Επιληψία	<input type="checkbox"/> Νεφρική Ανεπάρκεια
<input type="checkbox"/> Καρδιακή Ανεπάρκεια	<input type="checkbox"/> Δυσκολία κατάποσης	<input type="checkbox"/> Νοσητική ασθένεια	<input type="checkbox"/> Σακχ. Διαβήτης
<input type="checkbox"/> Εμφράγματα		Είδος νοσητικής ασθένειας:	<input type="checkbox"/> Καταρράκτης
<input type="checkbox"/> Μυοκαρδιοπάθεια			<input type="checkbox"/> Γλαύκωμα
<input type="checkbox"/> Πνευμονία			<input type="checkbox"/> Αρθρίτιδα
<input type="checkbox"/> Ασθμα			Είδος Αρθρίτιδας:
<input type="checkbox"/> Χ.Α.Π.			

Καταχωρήστε ό,τι άλλο σημαντικό ιατρικό γεγονός δεν υπάρχει παραπάνω που πρέπει (όπως εγχειρήσεις, άλλες ασθένειες κλπ)

Εγγραφή: 14 1 από 1

Εικόνα 2.2: Παράδειγμα ηλεκτρονικού φακέλου ασθενή Πηγή: Διαδικτυακές Πηγές [7]

2.3 Συστήματα Ηλεκτρονικού Φακέλου Υγείας

Περισσότερο από 30 χρόνια γίνονται προσπάθειες για την ανάπτυξη υπολογιστικών εφαρμογών που να διαχειρίζονται τα κλινικά δεδομένα. Οι πρώτες προσπάθειες επικεντρώνονταν στη δημιουργία προτυπωμένων φορμών με συγκεκριμένα πεδία που έπρεπε να συμπληρωθούν από το γιατρό, όπως πεδία για τη διάγνωση, για τα προσωπικά δεδομένα του ασθενή (όνομα, επίθετο, ηλικία), την κλινική εξέταση (βάρος, ύψος, αρτηριακή πίεση, θερμοκρασία), τη φαρμακευτική αγωγή. Αφού τις συμπλήρωνε ο γιατρός (και κάποια πεδία ο νοσηλευτής), τις αναλάμβανε κάποιος διοικητικός υπάλληλος που τις μετέφερε στον υπολογιστή. Από κει και πέρα ο γιατρός μπορούσε να συμβουλευτεί το φάκελο του ασθενή στον υπολογιστή οποιαδήποτε στιγμή. Τέτοια συστήματα διατηρούνται ακόμη και σήμερα και, μάλιστα, σε πολλές περιπτώσεις (Αποστολάκης, 2002).

Σε πολλά τμήματα στα σύγχρονα ελληνικά νοσοκομεία, υπάρχουν προτυπωμένες φόρμες όπου εισάγονται διάφορα δεδομένα από τους γιατρούς και στη συνέχεια καταχωρούνται σε μια βάση δεδομένων από τους υπαλλήλους της γραμματείας. Πρόκειται για απλές βάσεις δεδομένων που είναι εγκατεστημένες σε ένα μόνο υπολογιστή, χωρίς να διασυνδέονται με τα υπόλοιπα τμήματα. Ωστόσο, η σύγχρονη τάση πιέζει για πιο δυναμικά συστήματα με ενεργή συμμετοχή όλων των χρηστών.

Ο ηλεκτρονικός φάκελος ασθενή (Electronic Patient Record - EPR) είναι “ένας ψηφιακά αποθηκευμένος φάκελος με σκοπό να υποστηριχτεί η φροντίδα υγείας του ατόμου εφ’ όρου ζωής, η έρευνα και η εκπαίδευση των επαγγελματιών υγείας”

Τον ηλεκτρονικό φάκελο διαχειρίζεται το σύστημα ηλεκτρονικού φακέλου ασθενή το οποίο “βοηθά στην πρόσβαση και στο διαμοιρασμό πληροφοριών στους επαγγελματίες υγείας με φιλικό τρόπο και ελέγχει την ασφάλεια των δεδομένων”. Σε πολλές περιπτώσεις χρησιμοποιείται εναλλακτικά και ο όρος ‘ηλεκτρονικός φάκελος υγείας’ (Electronic Health Record - EHR).

Σε σύγκριση με το χειρόγραφο, ο ηλεκτρονικός φάκελος υπερτερεί σε διάφορα σημεία. Προσφέρει γρήγορη πρόσβαση σε δεδομένα ανεξάρτητα από τη θέση που βρίσκεται ο χρήστης και επιτρέπει την άμεση διαχείρισή τους. Παράλληλα, καταγράφονται όλοι οι τύποι δεδομένων (κείμενο, αριθμοί, εικόνες και άλλα), δεν σβήνονται ούτε καταστρέφονται δεδομένα,

προστατεύονται οι συσχετίσεις τους και εφαρμόζονται όλοι οι κανόνες προστασίας. Επιπλέον, οι πληροφορίες μπορούν να αναλυθούν και να βοηθήσουν στη λήψη μιας απόφασης (Αποστολάκης, 2002).

Με τη μέγιστη δυνατή διαχείριση των πόρων του συστήματος η παροχή φροντίδας υγείας γίνεται ποιοτικότερη. Άλλωστε, είναι δεδομένο ότι ένα αξιόπιστο και εύχρηστο αυτοματοποιημένο σύστημα που προσαρμόζεται εύκολα στις ανάγκες των χρηστών, γνωρίζει εύκολα την αποδοχή τους και προσφέρει ικανοποίηση στους επαγγελματίες υγείας η οποία περνά στους ασθενείς. Όταν, μάλιστα, υποστηρίζονται άρτια και κάποιες διοικητικές λειτουργίες (αποζημιώσεις, προγραμματισμός, διαχείριση πόρων), τότε έχουμε πλήρη συστήματα με πολύ μεγάλα οφέλη.

2.4 Χρήσεις Ηλεκτρονικού Φακέλου Υγείας

Η προφανής χρήση του ηλεκτρονικού φακέλου ασθενή, δηλαδή η φροντίδα υγείας του ασθενή και η άσκηση της κλινικής πράξης παραμένει ίδια με εκείνη του παραδοσιακού χειρόγραφου φακέλου ασθενή. Ωστόσο, ο ηλεκτρονικός φάκελος έχει και πολλές άλλες χρήσεις.

Τα σύγχρονα συστήματα ηλεκτρονικού φακέλου δεν λειτουργούν αυτόνομα αλλά διασυνδέονται με άλλα υποσυστήματα του νοσοκομείου από τα οποία αντλούν σημαντικά δεδομένα. Κατ' αυτό τον τρόπο τα εργαστηριακά δεδομένα ενσωματώνονται αυτόματα στο σύστημα και ο γιατρός μπορεί να έχει άμεση αντίληψη της κατάστασης ενός ασθενή. Είναι αυτονόητο ότι αντίστοιχη εσωτερική διασύνδεση υπάρχει και με τα υπόλοιπα τμήματα του νοσοκομείου που παράγουν δεδομένα για τον ασθενή, όπως το ακτινολογικό.

Ιδιαίτερα σημαντική είναι η χρήση του ηλεκτρονικού φακέλου ως διοικητικό εργαλείο. Καταρχήν δίνει τη δυνατότητα τόσο για αναφορά σε προηγούμενες επισκέψεις του ασθενή στο νοσοκομείο, όσο και για προγραμματισμό των επόμενων. Μάλιστα, ο προγραμματισμός από το σύστημα δεν είναι τυχαίος, καθώς συνυπολογίζει διάφορους παράγοντες πριν επικυρώσει το ραντεβού, όπως τη διαθεσιμότητα του γιατρού που κουράρει το συγκεκριμένο ασθενή ή την αναγκαιότητα επανάληψης μιας εξέτασης σε συγκεκριμένο χρονικό διάστημα (αξονική τομογραφία σε ένα καρκινοπαθή). Επίσης, κάθε γιατρός μπορεί να δει το ημερήσιο, εβδομαδιαίο ή και μηνιαίο πρόγραμμά του πατώντας απλώς ένα πλήκτρο, οπότε λαμβάνει μια εκτυπωμένη λεπτομερή αναφορά με τους ασθενείς που πρέπει να δει. Με αυτό τον τρόπο προγραμματίζει και

τις υπόλοιπες δραστηριότητές του. Ο συγκεκριμένος προγραμματισμός γίνεται από ειδικά προγράμματα λογισμικού που είτε ενσωματώνονται στο σύστημα του φακέλου, είτε λειτουργούν αυτόνομα και χρησιμοποιούν το φάκελο ως πηγή δεδομένων (Αποστολάκης, 2002).

Επιπλέον, με την ενσωμάτωση ή τη διασύνδεση στο σύστημα του ηλεκτρονικού φακέλου διάφορων λογιστικών προγραμμάτων, είναι δυνατόν να παράγονται αυτόματες τιμολογήσεις των ιατρικών πράξεων, των εργαστηριακών εξετάσεων, της νοσηλείας και των λοιπών κινήσεων του ασθενή στο νοσοκομείο και, επίσης, να τυπώνονται σχετικές αναφορές. Αν, μάλιστα, υπάρχει εξωτερική διασύνδεση με τις ασφαλιστικές εταιρείες και τα ταμεία, οι φορείς αυτοί ενημερώνονται αυτόματα και αποζημιώνουν το νοσοκομείο. Με την ηλεκτρονική διευθέτηση των οικονομικών εκκρεμοτήτων μειώνονται τα λάθη, καθώς υπάρχει πολλαπλός έλεγχος, εξοικονομείται χρόνος και όλοι οι φορείς αποζημιώνονται γρηγορότερα.

Μια άλλη περίπτωση εξωτερικής διασύνδεσης του συστήματος ηλεκτρονικού φακέλου είναι με αντίστοιχα συστήματα άλλων νοσοκομειακών ιδρυμάτων και φορέων υγείας, ώστε όχι μόνο να ενημερώνονται για κάποιον ασθενή, αλλά και να μπορούν να αξιοποιήσουν τα διαθέσιμα στοιχεία ποικιλοτρόπως, όπως με τη στατιστική επεξεργασία τους για ερευνητικούς σκοπούς. Βέβαια, η επεξεργασία των δεδομένων και η παραγωγή νέας γνώσης μπορεί να πραγματοποιηθεί και μέσα στον οικείο χώρο του νοσοκομείου που λειτουργεί το σύστημα.

Μια ακόμη δυνατότητα που προσφέρουν πολλά συστήματα είναι η ενσωμάτωση συστημάτων υποστήριξης της απόφασης και η σύνδεση με άλλες πηγές γνώσης. Τα συστήματα υποστήριξης της απόφασης λαμβάνουν τα δεδομένα ενδιαφέροντος, παράγουν μηνύματα ενημέρωσης ή προειδοποίησης (μπορεί να παράγουν ακόμη και e-mail) και βοηθούν το γιατρό στη λήψη αποφάσεων βελτιώνοντας την ποιότητα της φροντίδας υγείας. Η πρόσβαση σε πηγές ιατρικής γνώσης ποικίλει και περιλαμβάνει την πρόσβαση σε βάσεις δεδομένων στον Παγκόσμιο Ιστό (Medline, Pub Med, Medscape) καθώς και σε πηγές πληροφοριών που είναι ενσωματωμένες στο σύστημα του ηλεκτρονικού φακέλου.

Τέλος, με τον ηλεκτρονικό φάκελο επιτυγχάνεται η μελέτη της σχέσης κόστους- οφέλους των παρεχόμενων υπηρεσιών και η συνακόλουθη αξιολόγηση της αποτελεσματικότητας του συστήματος.

2.5 Πλεονεκτήματα - Μειονεκτήματα Ηλεκτρονικού Φακέλου Υγείας

Ένας ολοκληρωμένος ΗΦΥ, έχει (ή θα έπρεπε να έχει) τα παρακάτω χαρακτηριστικά, όπως υποστηρίζουν οι Gunter και Terry (2005):

- Βελτιώνει και διασυνδέεται με άλλες τεχνολογίες (τεχνολογίες μείωσης σφαλμάτων (error-reducing) και περιορισμού κόστους (cost-saving)), όπως τα συστήματα υποστήριξης αποφάσεων.
- Βελτιώνει τη ροή δεδομένων υγείας με τη χρήση διαλειτουργικής και τυποποιημένης ονοματολογίας.
- Βελτιώνει την ποιότητα της υγειονομικής περίθαλψης διευκολύνοντας την ακριβή και έγκαιρη επικοινωνία μεταξύ των παρόχων.
- Αυτοματοποιεί την κοινοποίηση των δυσμενών περιστατικών και των ιατρικών λαθών τόσο στους ασθενείς όσο και στους διαχειριζόμενους στοιχείων σχετικών με την υγεία για την εξαγωγή στατιστικών συμπερασμάτων.
- Διευκολύνει την αξιόπιστη και παραγωγική ιατρική έρευνα και μελέτη.
- Παρέχει πληροφορίες διοικητικής, οικονομικής και στατιστικής φύσεως για τους ασθενείς, καθώς και πληροφορίες ποιοτικού ελέγχου της ιατροφαρμακευτικής περίθαλψης.

Ένα από τα σημαντικότερα οφέλη του ΗΦΥ είναι οι δυνατότητες που προσφέρει σχετικά με τη μείωση σφαλμάτων. Τα δεδομένα υγείας στην ηλεκτρονική τους μορφή, ελαχιστοποιούν τον κίνδυνο της εσφαλμένης ανάγνωσης μιας ιατρικής συνταγής που οφείλεται στο δυσανάγνωστο γραφικό χαρακτήρα ενός ιατρού. Παράλληλα, τα ηλεκτρονικά δεδομένα υγείας μεταφέρονται άμεσα και με ευκολία, ελαχιστοποιώντας κατά συνέπεια τα σφάλματα που προκύπτουν από αντιγραφές, ενώ συμβάλουν στην αποφυγή των καθυστερήσεων στην καταγραφή των ιατρικών συνταγών ή των αποτελεσμάτων εξετάσεων μέσω τηλεφωνικής επικοινωνίας, όπως επισημαίνουν οι Walker et al. (2005). Σύμφωνα με τους Shah et al. (2006), προσφέρεται, επίσης η δυνατότητα καταγραφής συναρτήσεων για την επισήμανση, εκ των προτέρων, αλλεργικών αντιδράσεων ή άλλων ανακολουθιών σε μια προβλεπόμενη θεραπεία, ελαχιστοποιώντας την περίπτωση λάθους. Οι Margaret Caudill-Slosberg και Weeks (2005) αναφέρουν, ωστόσο, πως τα παραπάνω πλεονεκτήματα δεν είναι απόλυτα, καθώς υφίσταται

πάντα ο κίνδυνος ύπαρξης πρόσθετων δυσμενών γεγονότων, που οφείλονται στη λανθασμένη χρήση της τεχνολογίας από τον άνθρωπο,

Η χρήση του ΗΦΥ επιτρέπει τον έλεγχο των καταχωρήσεων στα αρχεία του ασθενούς, προκειμένου να είναι σε θέση να προειδοποιήσει τους ιατρούς σε περιπτώσεις όπου απαραίτητα δεδομένα έχουν παραληφθεί ή όπου οι προβλεπόμενες διαδικασίες δεν έχουν εκτελεστεί. Συγκεκριμένοι τύποι δεδομένων, όπως αποτελέσματα εργαστηριακών εξετάσεων ή ψηφιοποιημένων εξετάσεων είναι δυνατό να εισαχθούν στο αρχείο του ασθενούς αυτόματα. Οι ασθενείς έχοντας πρόσβαση στους ΗΦΥ τους (δικαίωμα ανάγνωσης μόνο των δεδομένων) από τον προσωπικό τους υπολογιστή έχουν τη δυνατότητα ελέγχου των καταχωρήσεων σε αυτούς, όπως ελέγχουν τις χρεώσεις στην πιστωτική τους κάρτα ή στον τραπεζικό τους λογαριασμό.

Η εκπαίδευση και η επικοινωνία αποτελούν περαιτέρω πλεονεκτήματα της χρήσης του ΗΦΥ. Οι ιατροί και οι ασθενείς χρησιμοποιούν τις ηλεκτρονικές καταχωρήσεις ώστε να μπορούν να αναπαριστούν σε γραφήματα το ιατρικό ιστορικό και την εξέλιξη της κατάστασης του ασθενούς. Τα συστήματα ηλεκτρονικού φακέλου είναι δυνατό να προγραμματιστούν ώστε να αποστέλλουν υπενθυμίσεις στους ασθενείς για συγκεκριμένα ζητήματα υγείας. Μηνύματα ηλεκτρονικού ταχυδρομείου αποστέλλονται από τους παρόχους υπηρεσιών υγείας προκειμένου να ενημερώνουν τους ασθενείς για νέες εξελίξεις στα θέματα υγείας που τους απασχολούν, για τα ιατρικά ραντεβού τους ή για φάρμακα που αποσύρονται από την αγορά. Είναι γεγονός πως οι ασθενείς χρησιμοποιούν σε όλο και μεγαλύτερο βαθμό το Διαδίκτυο προκειμένου να ενημερωθούν για θέματα που σχετίζονται με την υγεία, όπως εναλλακτικές θεραπείες, ή προς εύρεση ιατρών που ειδικεύονται στην πάθησή τους. Διαθέτοντας τον προσωπικό ΗΦΥ τους και με την καθοδήγηση των προσωπικών τους ιατρών, οι ασθενείς μπορούν να κάνουν καλύτερη χρήση της συγκεκριμένης πηγής πληροφοριών, όπως υποστηρίζει ο Deshpande και Jadad (2006).

Οι ασθενείς δεν εξαρτώνται από την γεωγραφική τους θέση και μπορούν να αλλάξουν ιατρό με μεγαλύτερη ευκολία ανάλογα με την ασφάλιση και τις προτιμήσεις τους. Αν, για παράδειγμα, τα αποτελέσματα των εξετάσεων από μια προγενέστερη θεραπεία είναι άμεσα διαθέσιμα σε ακριβή και ασφαλή μορφή στον ΗΦΥ, οι ασθενείς θα αποφύγουν την επανάληψη των εξετάσεων που απαιτούνται όταν θα θελήσουν να επισκεφτούν ένα νέο ιατρό που δεν γνωρίζει το ιστορικό τους.

Τα συστήματα ΗΦΥ μπορούν να εξυπηρετήσουν κρίσιμους σκοπούς της δημόσιας υγείας. Είναι δυνατό μέσω αυτών να ανιχνευθούν, για παράδειγμα, εξαπλώσεις επιδημιών. Συνεπώς, τα οφέλη ενός ΗΦΥ σε αντιδιαστολή με τις εγγραφές σε χαρτί, είναι τα ακόλουθα:

- Για τους ασθενείς:
 - Μείωση των ιατρικών σφαλμάτων.
 - Μείωση των περιπτώσεων δυσμενών αλληλεπιδράσεων φαρμάκων, καθώς και των αλλεργικών αντιδράσεων.
 - Επαλήθευση της ακρίβειας των δεδομένων που περιέχονται στον ΗΦΥ από τους ασθενείς.
 - Ενδυνάμωση της επικοινωνίας του ασθενούς με τους παρόχους υπηρεσιών υγείας.
 - Βελτίωση της κατανόησης των σχετικών με την υγεία θεμάτων.
 - Αποφυγή υποβολής του ασθενούς σε εξετάσεις περισσότερες από μια φορές.
- Για τους παρόχους υπηρεσιών υγείας:
 - Αύξηση της γνώσης σε ζητήματα πιθανών αλληλεπιδράσεων μεταξύ των φαρμάκων, καθώς και αλλεργικών αντιδράσεων.
 - Δυνατότητα παροχής πρόσβασης στα ιατρικά δεδομένα σε άλλους ιατρούς, όταν αυτό απαιτείται, καθώς επίσης και στους ίδιους τους ασθενείς.
 - Παροχή πληροφοριών στους ασθενείς για ζητήματα υγειονομικής περίθαλψης και υπηρεσιών υγείας.
 - Συνεχής παρακολούθηση της πορείας της υγείας του ασθενή και αξιολόγηση των κινδύνων.
 - Διευκόλυνση στην διεξαγωγή μελετών και ερευνών με τη δημιουργία βάσεων δεδομένων.
 - Παροχή έτοιμης λίστας φαρμάκων και παθήσεων.
- Για τους διαχειριζόμενους οικονομικά και οργανωτικά ζητήματα που σχετίζονται με τη υγεία:
 - Βελτίωση των υπηρεσιών εξυπηρέτησης των ασθενών σχετικά με τις διαδικασίες συναλλαγών και την παροχή πληροφοριών.

- Βελτίωση της διαχείρισης των οικονομικών ζητημάτων σχετικά με την ασφάλιση των ασθενών.
- Ανάλυση δεδομένων και εξαγωγή στατιστικών στοιχείων.
- Μείωση κόστους λειτουργίας νοσηλευτικών ιδρυμάτων
- Ανίχνευση επιδημιών και κινδύνων που απειλούν τη δημόσια υγεία.
- Συλλογή δεδομένων που χρησιμοποιούνται για βελτίωση ποιότητας, διαχείριση ρίσκου, σχεδιασμό πόρων, διαχείριση απόδοσης.

Όπως και κάθε νέα πρωτοβουλία, η χρήση του ΗΦΥ ενέχει και κάποιες δυσκολίες-εμπόδια. Τα εμπόδια αυτά είναι αναγκαίο να ξεπεραστούν έτσι ώστε να μπορέσουμε να κάνουμε βέλτιστη χρήση του ΗΦΥ και των δυνατοτήτων του.

Σύμφωνα με τις Αραποστάθη και Τζεμπετζή (2004), στα βασικά μειονεκτήματα συγκαταλέγεται το υψηλό κόστος και το εξειδικευμένο προσωπικό καθώς η εφαρμογή του ΗΦΥ αυξάνει τις δαπάνες για τη συγκεκριμένη επένδυση, το κόστος εγκατάστασης και συντήρησης του συστήματος, το κόστος εκπαίδευσης των χρηστών και επηρεάζει τα αναμενόμενα οφέλη. Η εισαγωγή στοιχείων απαιτεί περισσότερο χρόνο καθώς απαιτείται ειδική εκπαίδευση στον τρόπο καταγραφής και εισαγωγής των πληροφοριών που συλλέγονται αλλά και στον τρόπο επεξεργασίας τους.

Οι κίνδυνοι που υπάρχουν κατά τη χρησιμοποίηση του ηλεκτρονικού φακέλου περιγράφονται παρακάτω:

- ❖ Εξωτερικές παρεμβάσεις, με σκοπό την ανάγνωση, την κλοπή ή την παραποίηση των δεδομένων
- ❖ Διαρροή στοιχείων
- ❖ Χάσμα στα δεδομένων ραγδαία και απότομα (φυσικός κίνδυνος)
- ❖ Συλλογή δεδομένων για ερευνητικούς λόγους χωρίς εξουσιοδότηση
- ❖ Χάνεται η διαπροσωπική σχέση με τον ασθενή [3]

Άλλα μειονεκτήματα που παρουσιάζονται κατά την εφαρμογή του ηλεκτρονικού φακέλου αφορούν την ασφάλεια και την εμπιστευτικότητα. Αποτελούν σημαντικά εμπόδια στη διαδεδομένη εφαρμογή των συστημάτων ηλεκτρονικού φακέλου και στη διανομή στοιχείων.

Άλλο ζήτημα ίσης σπουδαιότητας είναι και η προστασία του χώρου που χρησιμοποιεί συστήματα ηλεκτρονικού φακέλου. Κανένα νοσηλευτικό ίδρυμα δεν θα είναι πρόθυμο να μοιραστεί τα στοιχεία του εάν μπορούν να χρησιμοποιηθούν για να παρέχουν ένα επιχειρησιακό πλεονέκτημα σε ανταγωνιστή.

Τέλος η επιτυχία της εφαρμογής του συστήματος ΗΦΥ εξαρτάται σε μεγάλο ποσοστό από το βαθμό αποδοχής και χρήσης του από το κλινικό προσωπικό. Η δυσπιστία με την οποία αντιμετωπίζεται η υιοθέτηση του συστήματος ΗΦΥ κυρίως από το μεγαλύτερο σε ηλικία προσωπικό που κατά βάση δεν έχει γνώσεις περί τεχνολογιών πληροφορίας και επικοινωνιών καθιστά την όλη προσπάθεια εφαρμογής ενός ηλεκτρονικού συστήματος ιατρικών φακέλων αρκετά πιο δυσχερές. Παρόλα τα μειονεκτήματα που παρουσιάζει ο ηλεκτρονικός φάκελος, υπάρχει ολοένα και αυξημένη ανάγκη για εφαρμογή του σε κλινικό επίπεδο.

Κεφάλαιο 3

Ασφάλεια και Νομοθετικό Πλαίσιο

3.1 Ασφάλεια Ηλεκτρονικού Φακέλου Υγείας

Ο όρος ασφάλεια συνοψίζει ένα ευρύ σύνολο θεμάτων που πρέπει να μελετηθούν σε ένα πληροφοριακό σύστημα υγείας. Ενδεικτικά, αναφέρεται το ιατρικό απόρρητο, η ιδιωτικότητα των προσωπικών δεδομένων, και η κρισιμότητα των ιατρικών εφαρμογών που οδηγεί σε αυξημένες ανάγκες για προστασία των υπολογιστικών συστημάτων από καταστροφές και για τακτική τήρηση αντιγράφων ασφαλείας.

3.1.1 Απειλές Πληροφοριακών Συστημάτων Υγείας

Με τον όρο απειλή κατά της ασφάλειας ενός Υπολογιστικού Συστήματος ορίζεται η πιθανή εκμετάλλευση μιας ευπάθειας του συστήματος με δυνητικό κίνδυνο την μη εξουσιοδοτημένη πρόσβαση, την αποκάλυψη πληροφοριών, την χρήση, την κλοπή ή την καταστροφή των πόρων του συστήματος.

Στα πλαίσια οποιουδήποτε συστήματος ή εφαρμογής ηλεκτρονικής υγείας είναι σημαντικό να εξασφαλιστεί το γεγονός ότι τα προσωπικά δεδομένα διατηρούνται ασφαλή και είναι διαθέσιμα στις οντότητες που έχουν πρόσβαση σε αυτά. Αυτό δεν είναι, ωστόσο, συχνά εύκολο να επιτευχθεί δεδομένου ότι πολλά δεδομένα παραδίδονται ή υποβάλλονται σε επεξεργασία μέσω των δικτύων, και ιδιαιτέρως μέσω του διαδικτύου.

1. Απειλές στην Εμπιστευτικότητα. Οι κακόβουλοι χρήστες που αποκτούν πρόσβαση στα προσωπικά δεδομένα υγείας των ασθενών αποτελούν σημαντική απειλή για την εμπιστευτικότητα στα ΠΣΥ. Η συγκεκριμένη απειλή ισχύει για τα δεδομένα που μεταφέρονται μέσω των δικτύων, καθώς επίσης και για τα δεδομένα που αποθηκεύονται στους εξυπηρετητές ενός ΠΣΥ.

Ως εκ τούτου, σύμφωνα με τους Dritsas et al. (2006) στο «A knowledge-based approach to security requirements for e-health applications», τα σημαντικότερα τμήματα ενός ΠΣΥ που υπόκεινται στις απειλές εμπιστευτικότητας είναι:

- το κανάλι επικοινωνίας μεταξύ του τερματικού εξοπλισμού του ασθενούς (π.χ. αισθητήρες) και του νοσοκομείου ή/και του εξοπλισμού του ιατρικού προσωπικού,
 - το κανάλι επικοινωνίας μεταξύ των εξυπηρετητών των ΠΣΥ και της εφαρμογής των τελικών χρηστών (ασθενών) και
 - τα στοιχεία που αποθηκεύονται στον εξυπηρετητή ενός ΠΣΥ ή τα στοιχεία που αποθηκεύονται στον εξοπλισμό των τελικών χρηστών (π.χ. ο προσωπικός υπολογιστής του ασθενούς).
2. Απειλές στην Ακεραιότητα. Η απειλή ενάντια στην ακεραιότητα των δεδομένων που μεταφέρονται ή αποθηκεύονται στο ΠΣΥ οδηγεί στη μεταβολή των δεδομένων αυτών από μη εξουσιοδοτημένους χρήστες. Όταν η συγκεκριμένη επίθεση πραγματοποιείται κατά τη διάρκεια των μεταδόσεων, οι νόμιμοι παραλήπτες λαμβάνουν δεδομένα διαφορετικά από αυτά που αποστέλλονται από τους δημιουργούς. Παράλληλα, η επίθεση μπορεί να πραγματοποιηθεί στα δεδομένα που βρίσκονται αποθηκευμένα στο σύστημα με αποτέλεσμα την τροποποίησή τους.
 3. Απειλές στην Αυθεντικότητα. Με την παραβίαση της αυθεντικότητας των δεδομένων στα ΠΣΥ, ένας κακόβουλος χρήστης μπορεί να πλαστογραφήσει ψευδή ιατρικά δεδομένα και να εξαπατήσει τους παραλήπτες στο ότι τα συγκεκριμένα δεδομένα προέρχονται από έναν διαφορετικό αποστολέα (τον οποίο ο παραλήπτης θεωρεί ως αυθεντικό). Αυτή η απειλή περιλαμβάνει την τροποποίηση τμήματος των δεδομένων που αποστέλλονται και συνήθως του τμήματος όπου προσδιορίζεται ο αποστολέας (header). Η αποποίηση είναι ένας παρόμοιος τύπος απειλής που εκφράζεται με την άρνηση της ιδιοκτησίας ή του περιεχομένου των δεδομένων που έχουν σταλεί. Ο αντίκτυπος αυτού του είδους των απειλών, που είναι δυνατό να οδηγήσουν σε πλαστογράφηση ιατρικών δεδομένων, μπορεί

να είναι τόσο σοβαρός ώστε να οδηγήσει σε καταστάσεις απειλής της ζωής των ασθενών (Dritsas et al., 2006).

4. Απειλές στη Διαθεσιμότητα. Απειλώντας τη διαθεσιμότητα ένας κακόβουλος χρήστης μπορεί να επηρεάσει το ΠΣΥ (ή ένα συγκεκριμένο τμήμα του) με τέτοιο τρόπο ώστε να παρακωλύει την προσφορά των προβλεπόμενων υπηρεσιών στους τελικούς χρήστες. Ο πιο κοινός τύπος της συγκεκριμένης απειλής είναι η επίθεση τύπου Denial of Service (DoS). Στις περιπτώσεις όπου οι πληροφορίες που παρέχονται μέσω του ΠΣΥ απαιτείται να είναι διαθέσιμες σε πραγματικό χρόνο, οι απειλές του τύπου αυτού έχουν σοβαρές συνέπειες σε ότι αφορά την υγεία των ασθενών.
5. Απειλές στην Ιδιωτικότητα. Πολλά είναι τα χαρακτηριστικά των ιατρικών δεδομένων που τονίζουν την υψηλή σημασία της ιδιωτικότητας στα ΠΣΥ (European Commission for Standardization, 2003). Το προφανέστερο είναι ο τύπος των δεδομένων που αποθηκεύεται και υποβάλλεται σε επεξεργασία στα περιβάλλοντα του τομέα της υγείας. Ένας χρήστης σε ένα περιβάλλον ΠΣΥ είναι δυνατό να μην γνωρίζει επακριβώς ποιες συσκευές και πότε τον ελέγχουν, τι είδους δεδομένα συλλέγουν, πού αποθηκεύονται τα δεδομένα αυτά, πού μεταφέρονται και ποιος έχει πρόσβαση σε αυτά ή μπορεί να τα επεξεργαστεί.

Οι απειλές στην ιδιωτικότητα στα πλαίσια ενός ΠΣΥ σχετίζονται με τις περιπτώσεις (Dritsas et al., 2006), όπου α) τα τμήματα των ΠΣΥ (π.χ. αισθητήρες) δρουν διαφανώς στους χρήστες, β) οι ενισχυμένες δυνατότητες αποθήκευσης παρέχουν ευκολότερη πρόσβαση, επεξεργασία και μεταφορά προσωπικών δεδομένων και δεδομένων υγείας, γ) η πρόοδος στις τεχνικές εξόρυξης δεδομένων (data mining) μπορεί να αυξήσει την ποσότητα και τον τύπο των προσωπικών δεδομένων που καταγράφονται και αναλύονται, δ) η μετάδοση δεδομένων σε ένα ΠΣΥ μπορεί να οδηγήσει στην αποκάλυψη προσωπικών δεδομένων

3.1.2 Απειλές Πληροφοριακών Συστημάτων Υγείας

3.1.2.1 Δέκα Βήματα για Ασφάλεια Πληροφοριακών Συστημάτων Υγείας

Οι υπηρεσίες ηλεκτρονικής υγείας στοχεύουν στη βελτίωση της ποιότητας ζωής. Η ασφάλεια, δηλαδή η προστασία της ακεραιότητας, διαθεσιμότητας, αυθεντικότητας και

εμπιστευτικότητας αλλά και η ιδιωτικότητα, δηλαδή η συμμόρφωση με τους κανονισμούς προστασίας προσωπικών δεδομένων, αποτελούν κρίσιμους παράγοντες για την επίτευξη της εμπιστοσύνης και της αποδοχής των ΠΣΥ από τους χρήστες. Παρακάτω παρουσιάζεται ένα βασικό σύνολο απαιτήσεων ασφάλειας και ιδιωτικότητας. Η νομική οντότητα Cyber Security Industry Alliance προτείνει τις παρακάτω απαιτήσεις για την ανάπτυξη και χρήση ενός αξιόπιστου ΠΣΥ.

- Ανάπτυξη ισχυρών ελέγχων αυθεντικοποίησης και εξουσιοδότησης. Η χρήση των ελέγχων αυθεντικοποίησης και εξουσιοδότησης, που περιλαμβάνουν ασφαλή ID tokens και ψηφιακά πιστοποιητικά, εξασφαλίζει το γεγονός ότι μόνο εξουσιοδοτημένοι χρήστες αποκτούν πρόσβαση σε ένα σύστημα και μόνο σε εκείνα τα τμήματα του συστήματος όπου απαιτείται, ώστε να εκτελέσουν τις εργασίες που επιθυμούν. Η χρήση των συνθηματικών δεν είναι αρκετή, καθώς μπορούν να αποκαλυφθούν με ευκολία. Η χρήση κατάλληλων μηχανισμών αυθεντικοποίησης και ελέγχων πρόσβασης προστατεύει όχι μόνο από τη μη εξουσιοδοτημένη πρόσβαση, αλλά παράλληλα μειώνει τον κίνδυνο μόλυνσης των συστημάτων από κακόβουλο λογισμικό (malware).
- Κρυπτογράφηση των δεδομένων και των επικοινωνιών. Τα δεδομένα που βρίσκονται αποθηκευμένα σε σκληρούς δίσκους, φορητούς υπολογιστές ή άλλες συσκευές αποθήκευσης πρέπει να προστατεύονται με ισχυρούς κρυπτογραφικούς μηχανισμούς. Ομοίως, τα δεδομένα υγείας πρέπει να προστατεύονται κατά τη μεταφορά τους από την μη εξουσιοδοτημένη παρακολούθηση. Η πρόκληση εντοπίζεται στην εφαρμογή ισχυρών κρυπτογραφικών μηχανισμών από άκρη σε άκρη, δηλαδή από το σπίτι του ασθενούς έως τα νοσοκομεία, ενώ συχνά μπορεί να καταλήγουν σε μια ασύρματη συσκευή όπως ένας υπολογιστής χειρός (PDA) ή ένα κινητό τηλέφωνο. Είναι γεγονός, ωστόσο, πως ήδη υφίστανται λύσεις ασφάλειας που επιτρέπουν την κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου και των βάσεων δεδομένων.
- Κατάλληλη διαχείριση του μη χρήσιμου εξοπλισμού και των δεδομένων. Καθώς τα δεδομένα τροποποιούνται, ενημερώνονται ή διορθώνονται, τα προηγούμενα στοιχεία πρέπει να εκκαθαριστούν με τέτοιο τρόπο που να αποτρέπει την ανάκτησή τους ή την πρόσβαση σε αυτά από μη εξουσιοδοτημένους χρήστες. Αυτό περιλαμβάνει την κατάλληλη διαχείριση ή καταστροφή των δεδομένων που βρίσκονται στις συσκευές μαζικής αποθήκευσης, στους εκτυπωτές και άλλες απομακρυσμένες συσκευές ή σε άλλες θέσεις από όπου οι μη εξουσιοδοτημένοι χρήστες θα μπορούν να τα ανακτήσουν.

- Έλεγχος των δεδομένων. Είναι γεγονός ότι όλο και περισσότερα δεδομένα εισάγονται στα συστήματα μέσω του ιστού δεδομένης της ανάγκης για απλές, διαλειτουργικές και εύκολα προσβάσιμες διεπαφές. Οι διεπαφές χρήστη πρέπει να υποστηρίζουν μια σύγχρονη υποδομή πληροφοριακών συστημάτων υγείας. Ωστόσο, παρουσιάζουν ευπάθειες, επιτρέποντας ενδεχομένως σε έναν επιτιθέμενο να αλλάξει ή να χειριστεί δεδομένα.
- Διενέργεια συχνών ελέγχων στο σύστημα. Όλες οι συναλλαγές πρέπει να ελέγχονται ώστε να διασφαλίζεται το γεγονός ότι αποκλειστικά οι εξουσιοδοτημένες και μόνο αυτές μπορούν να έχουν πρόσβαση και να μεταβάλλουν τα δεδομένα του συστήματος.
- Χρήση ψηφιακών υπογραφών και ασφαλών date-time stamps. Χρήση κρυπτογραφικών αθροισμάτων ελέγχου, δακτυλικών αποτυπωμάτων ή υπογραφών για να εξακριβωθεί ότι τα δεδομένα είτε κατά τη μεταφορά είτε κατά την αποθήκευσή τους σε μια βάση δεδομένων δεν έχουν τροποποιηθεί από μη εξουσιοδοτημένους χρήστες. Με τη χρήση των ψηφιακών υπογραφών οι υπογράφοι δεν μπορούν εκ των υστέρων να αρνηθούν την πρόσβαση ή τη χρήση των δεδομένων. Τα ασφαλή date-time stamps τεκμηριώνουν ακριβώς τη στιγμή που μια εγγραφή δημιουργήθηκε ή τροποποιήθηκε.
- Πλεονασμός. Όπως συμβαίνει με όλα τα συστήματα αποθήκευσης και ανάκτησης στοιχείων, υπάρχουν περιπτώσεις όπου τμήματα του Πληροφοριακού Συστήματος Υγείας δεν είναι διαθέσιμα εξαιτίας της αποτυχίας του υπάρχοντος εξοπλισμού, των επιθέσεων τύπου Denial of Service (DoS attacks) ή των προσχεδιασμένων παύσεων λειτουργίας. Ο πλεονασμός σε επίπεδο εισαγωγής δεδομένων, αποθήκευσης και ανάκτησης μειώνει ή εξαλείφει τα περισσότερα προβλήματα μη διαθεσιμότητας.
- Χρήση ιδιωτικού δικτύου κορμού. Οι διακοπές λειτουργίας των δικτύων λόγω των διακυμάνσεων στις ροές δεδομένων αποτελούν ένα συνεχές πρόβλημα. Ακόμα κι αν η πρόσβαση σε σημαντικά τμήματα του συστήματος από τους ασθενείς και τους επαγγελματίες πραγματοποιείται μέσω του διαδικτύου, το δίκτυο κορμού του συστήματος πρέπει να είναι ιδιωτικό κατά τρόπο παρόμοιο με εκείνους που χρησιμοποιούνται από τις τράπεζες και τους χρηματοδοτικούς οργανισμούς.
- Ανάπτυξη ενός μηχανισμού γρήγορης απόκρισης περιστατικών. Αναμφισβήτητα, τα Πληροφοριακά Συστήματα Υγείας αντιμετωπίζουν προβλήματα επιθέσεων, εισβολών και άλλων γεγονότων που έχουν επιπτώσεις στην ασφάλειά τους. Συχνά τα παραπάνω γεγονότα οδηγούν σε παύσεις λειτουργίας των συστημάτων ή καθυστερήσεις. Για την

αποφυγή ή τη μείωση της διάρκειας των περιόδων της μη διαθεσιμότητας των συστημάτων, απαιτείται η ενσωμάτωση ενός ισχυρού μηχανισμού απόκρισης περιστατικών στην αρχική ανάπτυξή τους. Απαιτείται, παράλληλα, η καθιέρωση μιας ομάδας διαχείρισης κρίσιμων καταστάσεων, κάθε μέλος της οποίας θα πρέπει να διαθέτει συγκεκριμένες αρμοδιότητες και υποχρεώσεις ώστε να δρα άμεσα.

- Εισήγηση δικτύων διαμοίρασης πληροφορίας. Η αξιόπιστη διαμοίραση πληροφοριών μεταξύ των διαχειριστών, των ειδικών στην ασφάλεια και των διευθυντών αποτελεί βασικό συστατικό ενός σωστά σχεδιασμένου πλάνου ασφάλειας πληροφοριών.

3.1.3 Ασφάλεια Ηλεκτρονικού Ιατρικού Φακέλου

Οι ιατρικές πληροφορίες για την υγεία ενός ατόμου αποτελούν προσωπικά δεδομένα, και επομένως όποιος έχει πρόσβαση σε αυτά δεν επιτρέπεται να τα χρησιμοποιεί για όφελος δικό του. Η τεχνολογία σήμερα έχει δώσει λύσεις για την ασφάλεια των ιατρικών δεδομένων, οι οποίες μάλιστα είναι περισσότερο ασφαλείς από αυτές που τηρούνταν μέχρι πριν λίγα χρόνια. Στον ηλεκτρονικό ιατρικό φάκελο πρέπει να δίδεται ιδιαίτερη έμφαση στην Προστασία των Προσωπικών Δεδομένων τα οποία θα αρχειοθετούνται (Καλιμάνη, 2013). Οι απαιτήσεις περιλαμβάνουν τα εξής επίπεδα:

- ❖ Οργανωτική Ασφάλεια
- ❖ Φυσική Ασφάλεια
- ❖ Ασφάλεια Υλικού
- ❖ Ασφάλεια Λειτουργικού Συστήματος
- ❖ Ασφάλεια Εφαρμογής

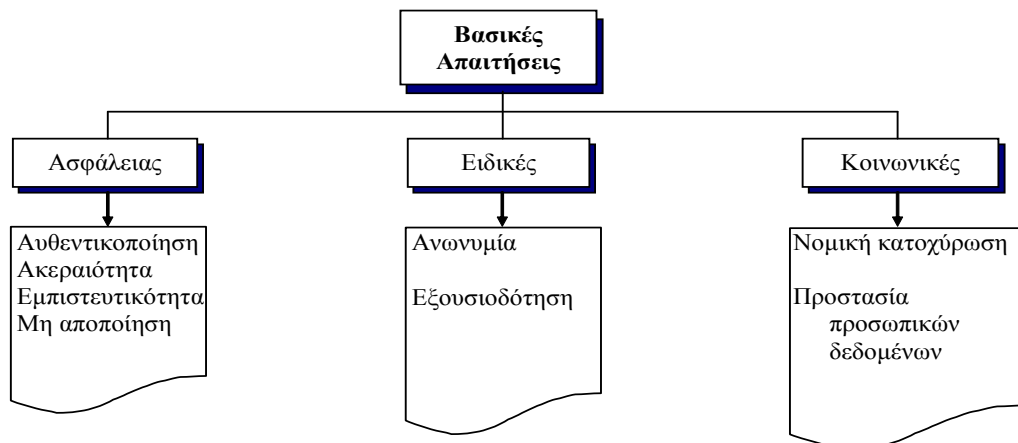
Είναι ξεκάθαρο ότι το δικαίωμα του ασθενούς για διασφάλιση της εμπιστευτικότητας των προσωπικών του δεδομένων δεν μπορεί να υποβιβασθεί εξαιτίας της χρήσης του ηλεκτρονικού φακέλου υγείας. Ο καθορισμός ηθικών και νομικών διαδικασιών και κριτηρίων όσο αφορά στην ηλεκτρονική συλλογή, επεξεργασία και διακίνηση των προσωπικών ευαίσθητων δεδομένων ασθενών σε πιθανούς χρήστες δεδομένων υγείας είναι απαραίτητος, αφού τυχόν αποκάλυψή τους θέτει σε κίνδυνο την σχέση τόσο ιατρού ή νοσηλεύτη - ασθενή, όσο και των μελών ολόκληρης της κοινωνίας αφού είναι πιθανό από τον φόβο αποκάλυψής τους, ο

ασθενής να μην εμπιστευθεί κρίσιμες πληροφορίες που αφορούν όχι μόνο στην υγεία του αλλά και στην διατήρηση της δημόσιας υγείας.

3.2 Ιδιωτικότητα, Εμπιστευτικότητα, Ακεραιότητα Ηλεκτρονικού Φακέλου Υγείας

3.2.1 Απαιτήσεις Ασφάλειας

Οι απειλές και οι ιδιαιτερότητες που παρουσιάζουν τα πληροφοριακά συστήματα υγείας οδηγούν στη στοιχειοθέτηση σαφών απαιτήσεων ασφάλειας για την αντιμετώπισή τους. Σε αυτή την ενότητα περιγράφονται οι απαιτήσεις αυτές όσον αφορά στην προστασία της ιδιωτικότητας.



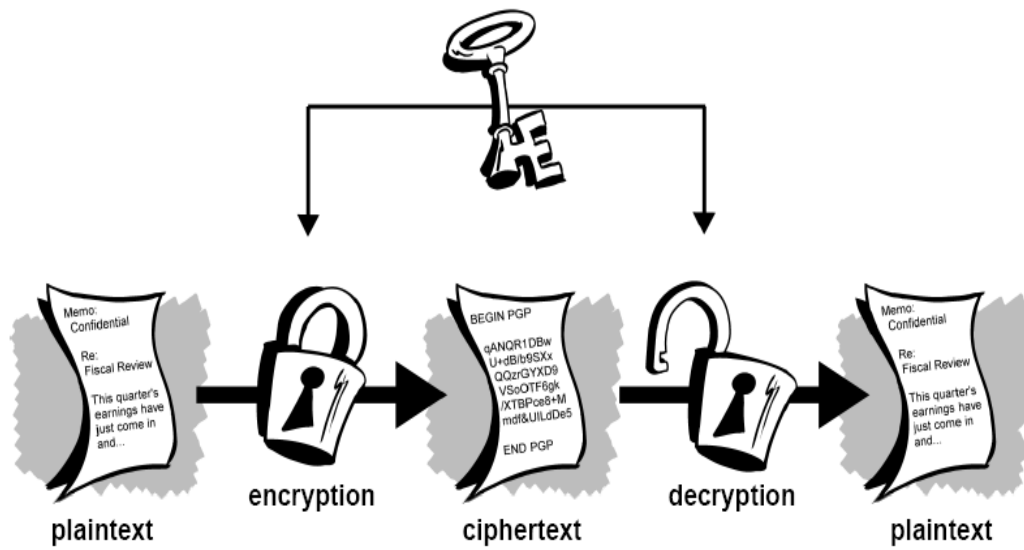
3.2.2 Εμπιστευτικότητα (Confidentiality)

Ως εμπιστευτικότητα ορίζεται η μη αποκάλυψη πληροφοριών σε χρήστες που δεν έχουν δικαίωμα ανάγνωσης της συγκεκριμένης πληροφορίας. Η εμπιστευτικότητα πολλές φορές ταυτίζεται με την προστασία της ιδιωτικότητας (Αποστολάκης, 2002). Όμως, παρόλο που η προστασία της ιδιωτικότητας προϋποθέτει την εμπιστευτικότητα, δεν αποτελεί ταυτόσημη έννοια καθώς για την προστασία της ιδιωτικότητας απαιτείται η πλήρωση και άλλων απαιτήσεων ασφάλειας.

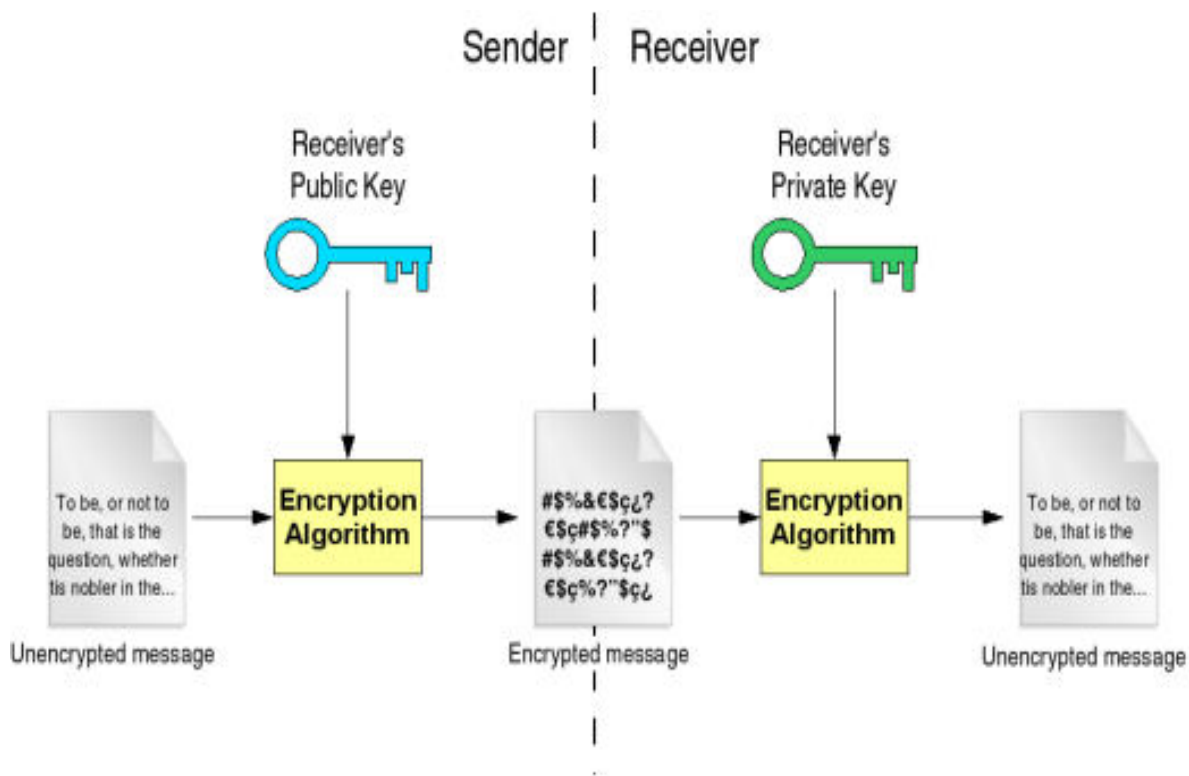
Η εμπιστευτικότητα προστατεύεται με διαδικασίες κρυπτογράφησης οι οποίες χωρίζονται σε τρεις κατηγορίες: συμμετρική κρυπτογράφηση, ασύμμετρη κρυπτογράφηση και συνδυασμός των δύο προηγούμενων μεθόδων. Η συμμετρική κρυπτογράφηση προϋποθέτει τη γνώση ενός κοινού μυστικού κλειδιού ανάμεσα στις οντότητες που επικοινωνούν και είναι γρήγορη υπολογιστικά μέθοδος. Τα κύρια προβλήματα της συμμετρικής κρυπτογράφησης είναι η διανομή των μυστικών κλειδιών και η διαχείριση των κλειδιών αυτών, καθώς χρειάζονται $n(n-1)/2$ κλειδιά για την επικοινωνία η κόμβων. Αντιθέτως, στην ασύμμετρη κρυπτογράφηση κάθε οντότητα κατέχει ένα ζεύγος κλειδιών, ένα δημόσιο και ένα ιδιωτικό. Προϋποθέτει υποδομή δημοσίου κλειδιού (Public Key Infrastructure — PKI) και είναι ευκολότερη μέθοδος όσον αφορά στη διαχείριση των κλειδιών καθώς χρειάζονται 2η κλειδιά για την επικοινωνία η κόμβων. Τα μειονεκτήματα της ασύμμετρης κρυπτογράφησης είναι το υπολογιστικό κόστος, το οποίο είναι μεγαλύτερο από το αντίστοιχο της συμμετρικής κρυπτογράφησης και η ανάγκη για Έμπιστη Τρίτη Οντότητα (Trusted Third Party - TTP). Ο συνδυασμός των παραπάνω μεθόδων κρυπτογράφησης ονομάζεται Ψηφιακός Φάκελος (Digital Envelope) και επιλύει τα προβλήματα διαμοιρασμού μυστικών κλειδιών που εμφανίζονται στη συμμετρική κρυπτογράφηση ενώ αντιμετωπίζει την υπολογιστική δυσκολία της ασύμμετρης κρυπτογράφησης. Τα μυστικά κλειδιά ανταλλάσσονται μέσω ασύμμετρης κρυπτογράφησης στην έναρξη της επικοινωνίας και στη συνέχεια χρησιμοποιείται συμμετρική κρυπτογράφηση.

Επίσης, η κρυπτογράφηση παρέχει υπηρεσίες αυθεντικοποίησης, ακεραιότητας και μη αποποίησης με χρήση διαφορετικών μηχανισμών για κάθε περίπτωση. Συνεπώς, η χρήση κρυπτογραφικών συστημάτων είναι απαραίτητη στον τομέα της πληροφορικής υγείας για την επίτευξη των παραπάνω απαιτήσεων ασφάλειας.

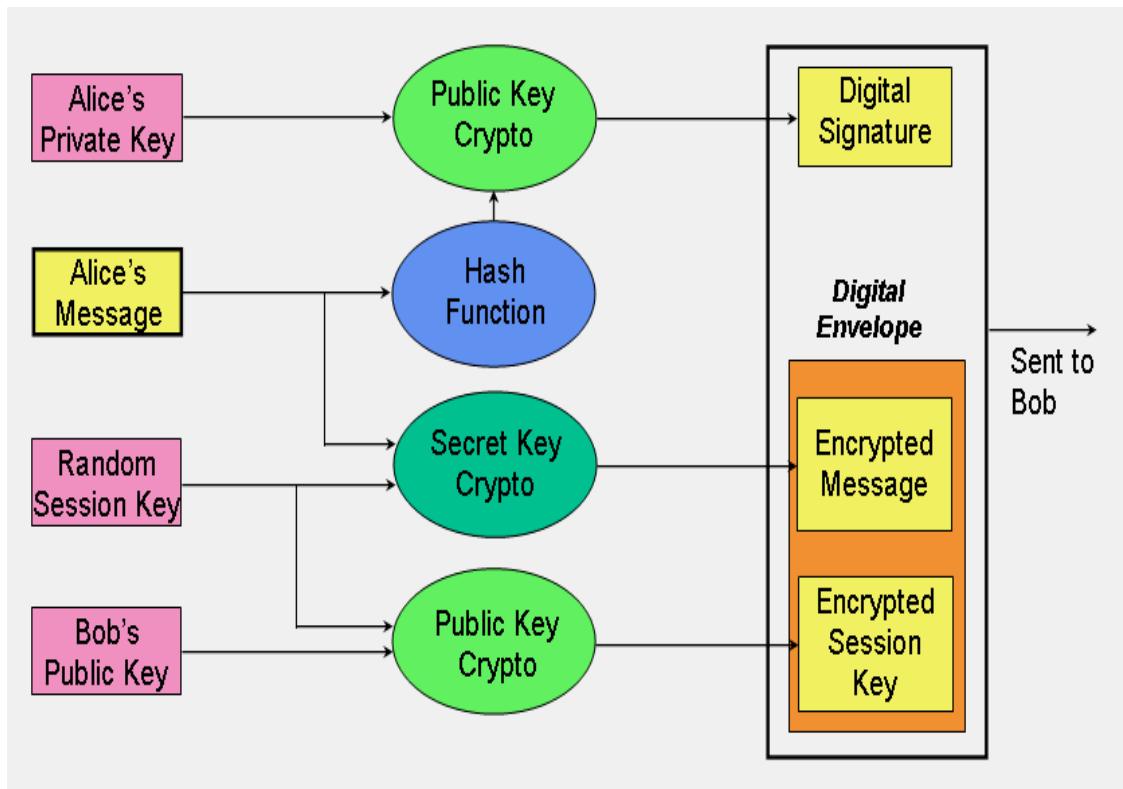
Η διατήρηση της εμπιστευτικότητας με χρήση των παραπάνω μηχανισμών κρυπτογράφησης προστατεύει από επιθέσεις κατά τις οποίες ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στα μηνύματα που ανταλλάσσονται ανάμεσα στους εξουσιοδοτημένους χρήστες και το πληροφοριακό σύστημα υγείας (eavesdropping attacks).



Εικόνα 3.1: Συμμετρικό κρυπτογραφικό σύστημα



Εικόνα 3.2: Ασύμμετρη κρυπτογραφία



Εικόνα 3.3: Συνδυασμός Συμμετρικής- Ασύμμετρης κρυπτογραφίας

3.2.3 Ακεραιότητα (Integrity)

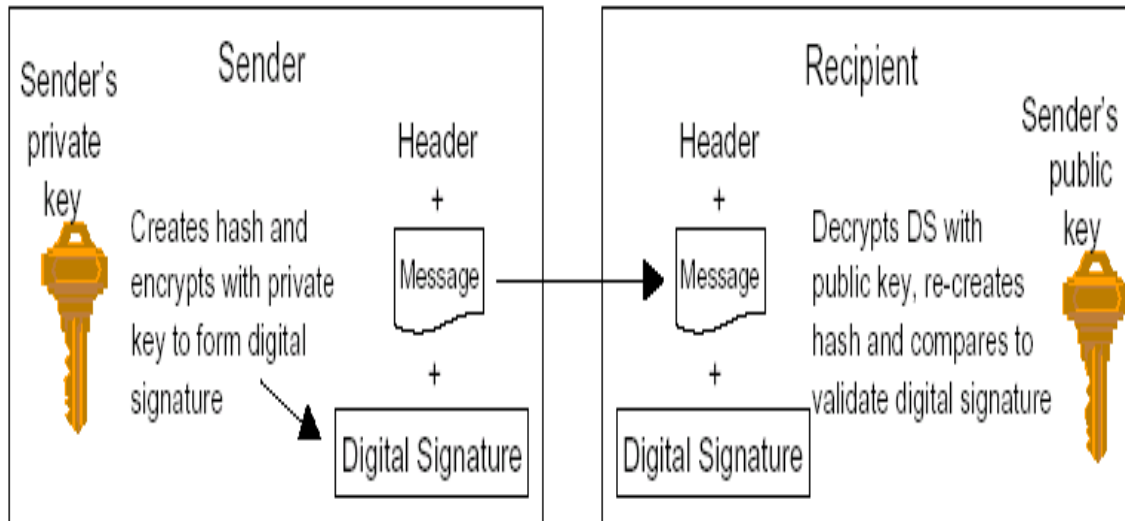
Οι διαδικασίες που εξασφαλίζουν την ακεραιότητα προφυλάσσουν το χρήστη από μηνύματα που έχουν αλλαχθεί είτε με την επέμβαση ενός κακόβουλου χρήστη/επιτιθέμενου είτε από αλλοιώσεις κατά την επικοινωνία, όπως για παράδειγμα από την επίδραση του θορύβου στο τηλεπικοινωνιακό μέσο. Στην πραγματικότητα δεν υπάρχει τρόπος να εμποδιστεί ή να διορθωθεί η αλλοίωση ενός μεταδιδόμενου μηνύματος όμως οι διαδικασίες που εξασφαλίζουν την ακεραιότητα των μεταδιδόμενων πληροφοριών βοηθούν τον παραλήπτη των δεδομένων να αναγνωρίσει πότε ένα μήνυμα έχει αλλοιωθεί (Αποστολάκης, 2002).

Στα πληροφοριακά συστήματα υγείας η ακεραιότητα δεν εφαρμόζεται μόνο στις μεταδιδόμενες πληροφορίες αλλά και στο περιεχόμενο του ηλεκτρονικού φακέλου ασθενή ως σύνολο, είτε κατά τη μετάδοσή του είτε κατά την αποθήκευση αυτού. Για παράδειγμα, θα πρέπει να αποτρέπεται η αλλοίωση των αποτελεσμάτων των ιατρικών εξετάσεων του ασθενούς.

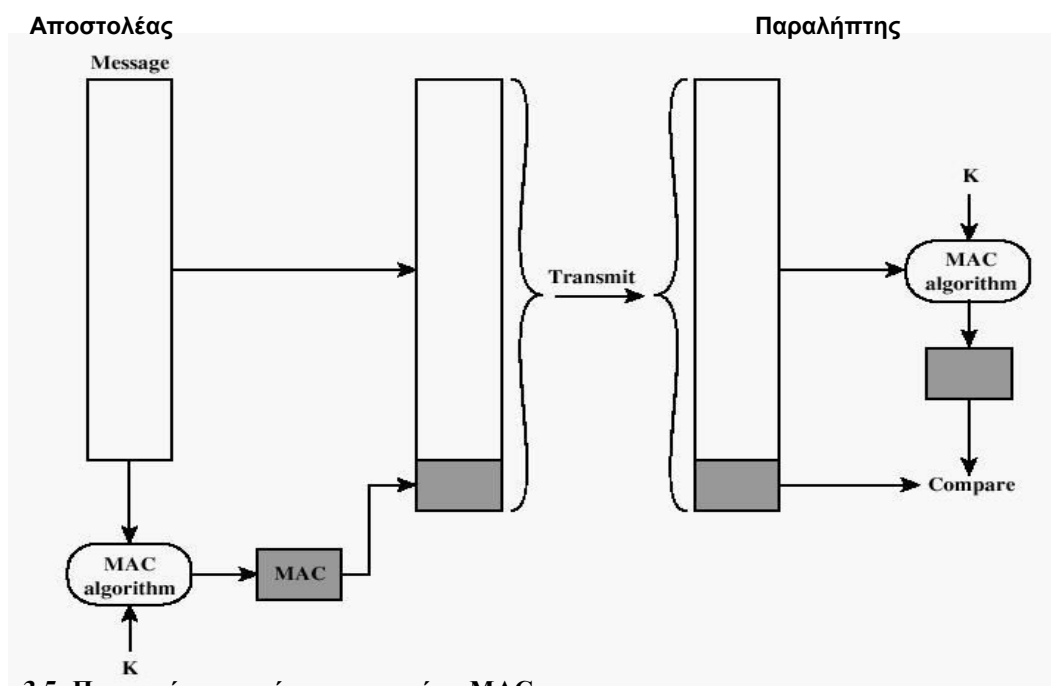
Ως απαίτηση ασφάλειας η ακεραιότητα δεν προφυλάσσει άμεσα την ιδιωτικότητα, όμως είναι απαραίτητη για την ασφαλή λειτουργία ενός πληροφοριακού συστήματος υγείας όπου οι πληροφορίες για την υγεία του ασθενούς δεν επιτρέπεται σε καμία περίπτωση να αλλοιωθούν.

Επιπλέον, οι τεχνολογίες που χρησιμοποιούνται για τη διασφάλιση της εμπιστευτικότητας, η οποία είναι ουσιώδης για την προστασία της ιδιωτικότητας, χρησιμοποιούνται συνήθως και για τη διασφάλιση της ακεραιότητας με μικρές διαφοροποιήσεις.

Πιο συγκεκριμένα, για την ακεραιότητα των μεταδιδόμενων πληροφοριών χρησιμοποιείται ο κώδικας αυθεντικοποίησης μηνύματος (Message Authentication Code - MAC) σε περιβάλλοντα συμμετρικής κρυπτογράφησης και οι ψηφιακές υπογραφές (Digital Signatures - DS) σε περιβάλλοντα ασύμμετρης κρυπτογράφησης. Το MAC αποτελεί την έξοδο μιας μονόδρομης συνάρτησης σύνοψης (Hash function), η οποία δέχεται ως είσοδο το μήνυμα και το μυστικό κλειδί κρυπτογράφησης. Ομοίως, η ψηφιακή υπογραφή είναι η έξοδος μιας hash συνάρτησης κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα. Η συνάρτηση hash στην περίπτωση της ψηφιακής υπογραφής δέχεται ως είσοδο το μήνυμα. Τόσο το MAC όσο και η ψηφιακή υπογραφή επισυνάπτονται και αποστέλλονται μαζί με το μήνυμα. Ο παραλήπτης, ο οποίος χρησιμοποιεί τις ίδιες συναρτήσεις σύνοψης, στην περίπτωση του MAC παράγει τη σύνοψη του μηνύματος που έλαβε σε συνδυασμό με το μυστικό κλειδί και συγκρίνει το αποτέλεσμα αυτό με το MAC που έλαβε. Αν το MAC που έλαβε είναι ακριβώς αυτό που παρήγαγε τότε το μήνυμα δεν έχει αλλοιωθεί κατά τη μετάδοση. Σε αντίθετη περίπτωση ζητάει την επανεκπομπή του μηνύματος. Ομοίως, στην περίπτωση όπου χρησιμοποιούνται ψηφιακές υπογραφές, ο παραλήπτης αποκρυπτογραφεί την ψηφιακή υπογραφή με το δημόσιο κλειδί του αποστολέα και παράγει τη σύνοψη του μηνύματος. Τέλος, συγκρίνει τη σύνοψη του μηνύματος που παρήγαγε με την αποκρυπτογραφημένη σύνοψη που έλαβε και αποφαινεται αν το μήνυμα έχει αλλοιωθεί κατά τη μετάδοση. Αξίζει να σημειωθεί πως τόσο το MAC όσο και η ψηφιακή υπογραφή αποδεικνύουν και την αυθεντικότητα του μηνύματος αφού μόνο ο αποστολέας μπορεί να γνωρίζει το μυστικό ή το ιδιωτικό του κλειδί αντίστοιχα. Τέλος, η ψηφιακή υπογραφή διασφαλίζει επιπλέον τη μη αποποίηση καθώς μόνο ο αποστολέας μπορεί να δημιουργήσει έγκυρη ψηφιακή υπογραφή με χρήση του ιδιωτικού του κλειδιού (Αποστολάκης, 2002).



Εικόνα 3.4: Δημιουργία και Επαλήθευση Ψηφιακής Υπογραφής



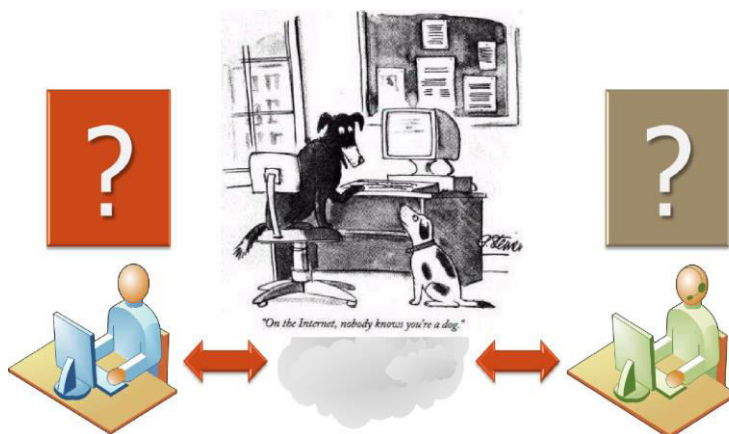
Εικόνα 3.5: Πιστοποίηση μηνύματος με χρήση MAC

3.2.4 Αυθεντικοποίηση (Authentication)

Η αυθεντικοποίηση αποτελεί διαδικασία κατά την οποία οι χρήστες αποδεικνύουν την ταυτότητά τους στο σύστημα και το αντίστροφο. Η απόδειξη αυτή πραγματοποιείται όταν η οντότητα που προσπαθεί να αυθεντικοποιηθεί παρέχει κάποια διαπιστευτήρια στην οντότητα που πραγματοποιεί την αυθεντικοποίηση. Τέτοια διαπιστευτήρια μπορούν να είναι: πληροφορίες που η οντότητα γνωρίζει (π.χ. password), αποδείξεις τις οποίες η οντότητα κατέχει (π.χ. smart card), κάποιο μοναδικό χαρακτηριστικό μιας φυσικής οντότητας (π.χ. δακτυλικό αποτύπωμα) ή οποιοσδήποτε συνδυασμός των παραπάνω. Ως απαίτηση ασφάλειας είναι ιδιαίτερα σημαντική καθώς εξασφαλίζει πως οι χρήστες οι οποίοι αποκτούν πρόσβαση στο σύστημα είναι εκείνοι που δηλώνουν. Η αυθεντικοποίηση δεν περιορίζεται στα φυσικά πρόσωπα αλλά επεκτείνεται σε μηχανήματα και διεργασίες του συστήματος. Επιπλέον, μπορεί να είναι αμφίδρομη ή μονοκατευθυντική (Αποστολάκης, 2002).

Η αυθεντικοποίηση προστατεύει από επιθέσεις κατά τις οποίες ο επιτιθέμενος προσπαθεί να μεταμφιεστεί σε νόμιμο χρήστη του συστήματος ή να προσποιηθεί ένα στοιχείο του συστήματος (spoofing/impersonation attacks).

Στα πληροφοριακά συστήματα υγείας η αυθεντικοποίηση αποτελεί ουσιώδη απαίτηση ασφάλειας καθώς ελλείψεις μηχανισμοί αυθεντικοποίησης μπορούν να επιτρέψουν την πρόσβαση μη εξουσιοδοτημένων χρηστών στα ευαίσθητα δεδομένα που τα συστήματα αυτά διαχειρίζονται με αποτέλεσμα την παραβίαση της ιδιωτικότητας.

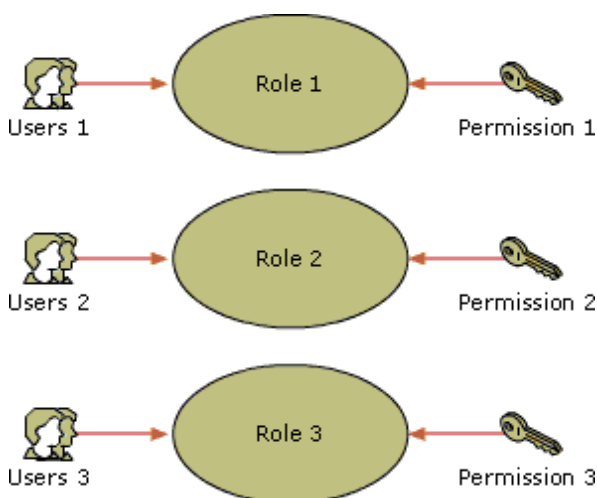
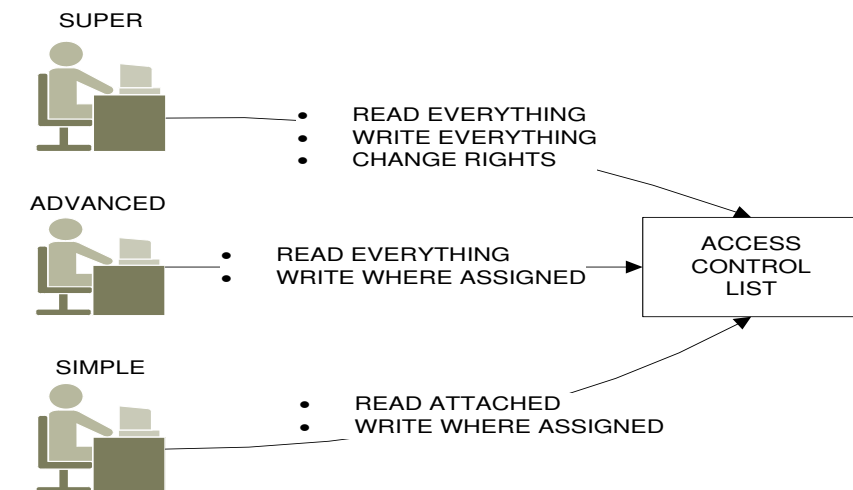


Αυθεντικοποίηση – πιστοποίηση ταυτότητας(authenticity)

3.2.5 Εξουσιοδότηση (Authorization)

Η εξουσιοδότηση αποτελεί το επόμενο στάδιο μετά τη διαδικασία της αυθεντικοποίησης. Όταν ένας χρήστης ή μια οντότητα αυθεντικοποιηθεί στο σύστημα δε σημαίνει απαραίτητα πως αποκτά πρόσβαση σε όλα τα δεδομένα που το σύστημα διαχειρίζεται. Για παράδειγμα, ο ιατρός δε μπορεί να έχει απεριόριστη πρόσβαση στον ηλεκτρονικό φάκελο του ασθενούς. Τα δικαιώματα που έχει κάθε χρήστης ή οντότητα καθορίζονται με τις διαδικασίες εξουσιοδότησης, οι οποίες προστατεύουν την ιδιωτικότητα καθώς διασφαλίζουν πως κάθε χρήστης θα έχει πρόσβαση μόνο στα δεδομένα που του επιτρέπονται (Αποστολάκης, 2002).

Η εξουσιοδότηση επιτυγχάνεται με τη χορήγηση δικαιωμάτων πρόσβασης τόσο σε κάθε οντότητα ξεχωριστά (entity-based) όσο και σε ομάδες οντοτήτων οι οποίες έχουν τον ίδιο ρόλο σε έναν οργανισμό (role-based).

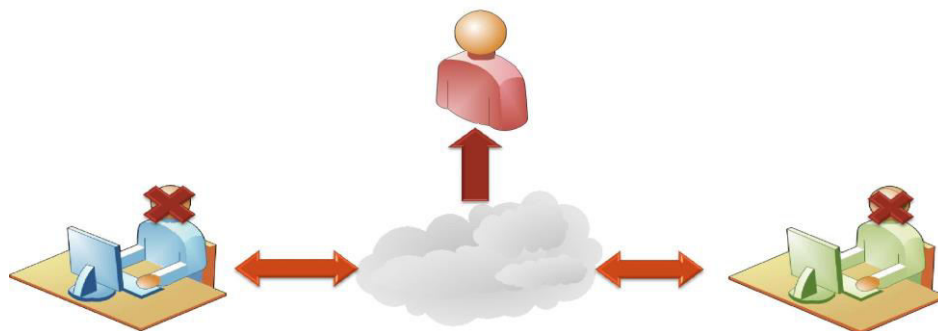


Εικόνα 3.6 : Δικαιώματα Χρηστών στην Πρόσβαση

3.2.6 Ανωνυμία (Anonymity)

Όπως αναλύθηκε σε προηγούμενη ενότητα, η νομοθεσία υποχρεώνει τους υπεύθυνους επεξεργασίας να ανωνυμοποιούν τα δεδομένα προκειμένου αυτά να διατεθούν σε ερευνητές ή ακόμα και κατά την οριοθέτηση τους στη βάση δεδομένων του συστήματος. Η ανωνυμοποίηση των δεδομένων δεν επιτρέπει την αναγνώριση του φυσικού προσώπου στο οποίο αναφέρονται τα δεδομένα (Αποστολάκης, 2002).

Απειλές κατά της ιδιωτικότητας όπως για παράδειγμα, η εξόρυξη δεδομένων (data mining) αποτρέπονται με ισχυρούς αλγόριθμους ανωνυμοποίησης.



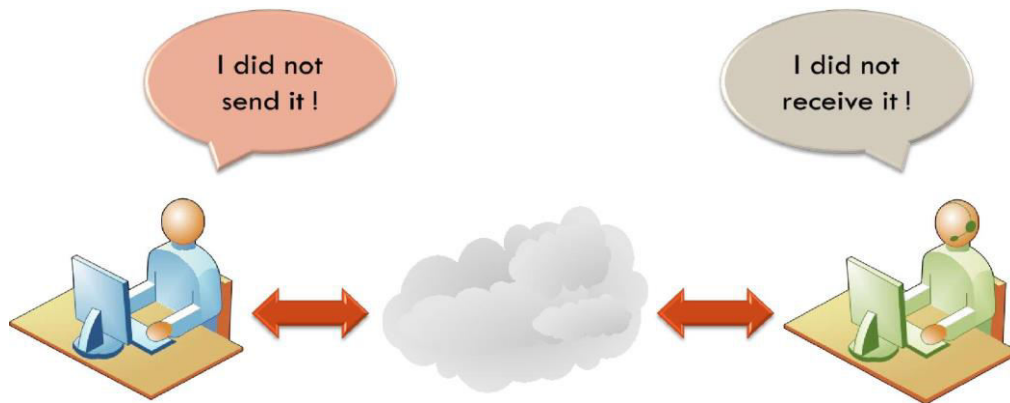
Ανωνυμία (anonymity)

3.2.7 Μη Αποποίηση (Non Repudation)

Στο χώρο της υγείας απαιτείται η απόδοση ευθυνών σε περίπτωση σφάλματος. Κάτι τέτοιο δε μπορεί να πραγματοποιηθεί αν κάθε χρήστης μπορεί να αποποιηθεί τη συμμετοχή του σε μία διαδικασία. Για το λόγο αυτό είναι απαραίτητο να υλοποιούνται μηχανισμοί μη αποποίησης των ενεργειών κάθε χρήστη στο σύστημα.

Η μη αποποίηση διαφυλάσσεται με μηχανισμούς ψηφιακής υπογραφής. Ο υπογράφων μία διαδικασία δε μπορεί να αποποιηθεί τη συμμετοχή του σε αυτή καθώς είναι ο μόνος που μπορεί να παράξει τη συγκεκριμένη ψηφιακή υπογραφή. Οι επιθέσεις μεταμφίεσης μπορούν να

αποφευχθούν με τη χρήση ψηφιακών υπογραφών ενώ κάθε αλλαγή στα περιεχόμενα του ιατρικού φακέλου θα πρέπει να υπογράφεται από τον χρήστη προκειμένου να μπορούν να αποδοθούν ευθύνες σε περίπτωση σφάλματος.



Μη αποποίηση συμμετοχής σε δοσοληψία(non-repudiation)

3.2.8 Καταγραφή Γεγονότων (Auditing)

Όπως σε κάθε πληροφοριακό σύστημα, έτσι και στα πληροφοριακά συστήματα υγείας απαιτείται η καταγραφή όλων των ενεργειών που πραγματοποιούνται από κάθε χρήστη με σκοπό την ανακάλυψη πιθανών κακόβουλων πράξεων. Στο χώρο της υγείας όμως η καταγραφή αυτών των πράξεων είναι ιδιαίτερως σημαντική καθώς μέσω της καταγραφής γεγονότων μπορούν να διαχειριστούν οι περιπτώσεις όπου χρειάζεται πρόσβαση στα δεδομένα χωρίς τη συγκατάθεση του ασθενούς, όπως για παράδειγμα σε περιπτώσεις ατυχήματος. Οι ιατροί αποκτούν πρόσβαση στον ηλεκτρονικό φάκελο του ασθενούς αλλά η ενέργειά τους αυτή καταγράφεται ώστε αργότερα να διαπιστωθεί αν ήταν πράγματι έννομη. Επίσης, με τη διαδικασία αυτή μπορούν εύκολα να αποδοθούν οι ευθύνες που βαραίνουν τους χρήστες.

Απειλές όπου ο κακόβουλος χρήστης χρησιμοποιεί τα δικαιώματα πρόσβασης που του παρέχονται χωρίς τη συγκατάθεση του ασθενούς ή γενικότερα με τρόπο που αντιβαίνει στην

πολιτική ασφάλειας του συστήματος, μπορούν να αντιμετωπιστούν με την καταγραφή γεγονότων με την προϋπόθεση πως τα log αρχεία του συστήματος ελέγχονται συστηματικά. Αξίζει να σημειωθεί πως η διαδικασία καταγραφής γεγονότων δεν αποτρέπει κακόβουλες συμπεριφορές αλλά επιτρέπει στους διαχειριστές του συστήματος να τις εντοπίσουν και να τις αντιμετωπίσουν.

3.2.9 Ενοποίηση Δεδομένων (Data Aggregation)

Η αιτία σχεδιασμού των συστημάτων τα οποία διαχειρίζονται ηλεκτρονικούς φάκελους ασθενών και η λειτουργικότητα των ηλεκτρονικών φακέλων αυτών είναι η ευκολία ενοποίησης των δεδομένων σε ηλεκτρονική μορφή σε αντίθεση με τα δεδομένα που βρίσκονται σε έντυπη μορφή. Όμως η ενοποίηση αυτή εγκυμονεί κινδύνους καθώς, αν εφαρμόζονται ελλιπή μέτρα ασφάλειας, μπορεί να πραγματοποιηθεί και αιτία για κακόβουλους χρήστες. Συνεπώς, η ενοποίηση των δεδομένων δεν αποτελεί απαίτηση ασφάλειας αλλά αναφέρεται εδώ γιατί ως διαδικασία δημιουργεί προβλήματα ασφάλειας και συνεπώς επηρεάζει το δικαίωμα της ιδιωτικότητας.

Το ίδιο ισχύει και με την εξόρυξη δεδομένων (data mining), η οποία είναι χρήσιμη ως λειτουργία στους χρήστες των πληροφοριακών συστημάτων υγείας για την εξαγωγή συμπερασμάτων σχετικά με την υγεία του ασθενούς αλλά αποτελεί επικίνδυνο εργαλείο όταν χρησιμοποιείται από κακόβουλους χρήστες.

3.3 Νομοθετικό Πλαίσιο

Το δικαίωμα στην ιδιωτικότητα κατοχυρώνεται τόσο σε διεθνές, όσο και σε εθνικό επίπεδο σε πολλές χώρες ανά τον κόσμο. Στο άρθρο 12 παράγραφος 1 της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα ορίζεται πως “κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους” (Οργανισμός Ηνωμένων Εθνών, 1948). Στο χώρο των πληροφοριακών συστημάτων η προστασία του δικαιώματος αυτού συνίσταται στην προστασία των προσωπικών δεδομένων και των πληροφοριών που εξάγονται από την επεξεργασία αυτών. Τα πληροφοριακά συστήματα υγείας και τα συστήματα διαχείρισης ηλεκτρονικού ιατρικού φακέλου επεξεργάζονται τέτοιου είδους δεδομένα και ως εκ τούτου η λειτουργία τους διέπεται από τις αντίστοιχες νομικές διατάξεις, οι οποίες άπτονται του δικαιώματος της ιδιωτικότητας και του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα.

3.3.1 Ελλάδα

Στην Ελλάδα το δικαίωμα της ιδιωτικότητας κατοχυρώνεται στο άρθρο 9 του Συντάγματος 1975/1986/2001 ενώ το δικαίωμα προστασίας των προσωπικών δεδομένων κατοχυρώνεται στο άρθρο 9 του Συντάγματος, το οποίο ορίζει πως “καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Επιμέρους νόμοι εξειδικεύουν το παραπάνω άρθρο και καθορίζουν το νομικό πλαίσιο για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και ειδικότερα των δεδομένων υγείας.

3.3.1.1 Νόμος 2472/1997

Ο Νόμος 2472/1997 αποτελεί εφαρμογή της Οδηγίας 95/46/EK (βλ. § 3.3.1) της Ευρωπαϊκής Ένωσης και στόχος του 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 1, εδάφιο 1). Ο Νόμος

ψηφίστηκε στις 26/03/1997 και τέθηκε σε ισχύ στις 10/04/1997 ενώ, μετέπειτα, τροποποιήθηκε από το Ν. 3471/2006, το Ν.2915/2001, το Ν.3156/2003 και το Ν.3625/2007.

Με την ψήφιση του Ν.2472/1997 θεσπίζεται μια ανεξάρτητη διοικητική Αρχή, η Αρχή Προστασίας Προσωπικών Δεδομένων (κεφ. Δ', άρθρο 17), η οποία έχει την εποπτεία της εφαρμογής του Νόμου αυτού καθώς και άλλων ρυθμίσεων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επίσης, γίνεται ορισμός των βασικών εννοιών και ορίζονται συγκεκριμένοι κανόνες σχετικά με την επεξεργασία των προσωπικών δεδομένων.

Πιο συγκεκριμένα:

- Δεδομένα προσωπικού χαρακτήρα νοούνται όλα τα δεδομένα που αφορούν το υποκείμενο των δεδομένων και μπορούν να το προσδιορίσουν μοναδικά. Σε αυτή την κατηγορία δεν εμπίπτουν τα δεδομένα στατιστικής φύσης, όταν η ταυτότητα του υποκειμένου δε μπορεί να προσδιοριστεί από αυτά (άρθρο 2, §).
- Ευαίσθητα δεδομένα ορίζονται όλα τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση του υποκειμένου, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική του ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων (άρθρο 2, § β5 μετά την τροποποίηση από τον Ν.3471/2006). Αξίζει να σημειωθεί πως τα δεδομένα που αφορούν στην υγεία δεν καθορίζονται σαφώς από το Ν. 2472/1997 ή την Οδηγία 95/46/ΕΚ. Παρόλα αυτά, η Σύσταση (97) 5 του Συμβουλίου της Ευρώπης διευκρινίζει πως δεδομένα υγείας θεωρούνται όλα τα δεδομένα που αφορούν την υγεία του ατόμου καθώς και τα δεδομένα που συνδέονται στενά με αυτή, όπως για παράδειγμα, η ειδικότητα του θεράποντος ιατρού.

Με την ανωτέρω διάκριση μεταξύ ευαίσθητων δεδομένων και δεδομένων προσωπικού χαρακτήρα γίνεται μια προσπάθεια αποτίμησης της αξίας των δεδομένων, η οποία είναι ανάλογη της φθοράς που υφίσταται το υποκείμενο από την αποκάλυψή τους. Τα ευαίσθητα δεδομένα αξιολογούνται ως πιο επικίνδυνα και αυτό οδηγεί σε μεγαλύτερους περιορισμούς σχετικά με την επεξεργασία τους.

Επεξεργασία δεδομένων προσωπικού χαρακτήρα ορίζεται κάθε εργασία που πραγματοποιείται με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε

δεδομένα προσωπικού χαρακτήρα, όπως η αποθήκευση, η συλλογή, η διάδοση, η τροποποίηση, η διασύνδεση και η καταστροφή (άρθρο 2, § δ').

Αρχείο δεδομένων προσωπικού χαρακτήρα (αρχείο) αποτελεί κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προσιτά με γνώμονα συγκεκριμένα κριτήρια (άρθρο 2, § ε5).

Η συγκεκριμένη παράγραφος του άρθρου 2 αντικατέστησε, σύμφωνα με την παράγραφο 2 του άρθρου 18 του Ν.3471/2006, το γενικότερο ορισμό του αρχείου ως "σύνολο δεδομένων προσωπικού χαρακτήρα που αποτελούν ή μπορούν να αποτελέσουν αντικείμενο επεξεργασίας". Η τροποποίηση, όπως σημειώνεται στην αιτιολογική έκθεση του νομοσχεδίου που οδήγησε στο Ν.3471/2006, αποτελεί έναν τεχνολογικά ουδέτερο ορισμό του αρχείου, ο οποίος, σε συνδυασμό με τον ορισμό της επεξεργασίας, εξασφαλίζει τη δυνατότητα διατήρησης ενός υψηλού επιπέδου προστασίας των δεδομένων και εναρμονίζεται καλύτερα με την Οδηγία 95/46/ΕΚ.

Διασύνδεση νοείται η επεξεργασία που συνίσταται στη δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα άλλων αρχείων που τηρούνται για άλλο σκοπό (άρθρο 2, § στ'). Κάθε διασύνδεση αρχείων πρέπει να γνωστοποιείται στην Αρχή από τους υπεύθυνους επεξεργασίας και στην περίπτωση που κάποιο από τα αρχεία περιλαμβάνει ευαίσθητα δεδομένα ή η διασύνδεση έχει ως συνέπεια την αποκάλυψη ευαίσθητων δεδομένων ή αν για την πραγματοποίηση της χρησιμοποιηθεί ενιαίος κωδικός, απαιτείται ειδική άδεια από την Αρχή (άρθρο 8, § 2-3).

Συγκατάθεση του υποκειμένου των δεδομένων ορίζεται κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή, και εν πλήρη επίγνωση, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί τουλάχιστον για το σκοπό της επεξεργασίας και τα δεδομένα που αφορά, τους αποδέκτες των δεδομένων καθώς και τα στοιχεία του υπεύθυνου επεξεργασίας, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα (άρθρο 2, § ια5).

Υπεύθυνος επεξεργασίας νοείται οποιοσδήποτε καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (άρθρο 2, § ζ'). Ο υπεύθυνος επεξεργασίας υποχρεούται να ελέγχει και να διατηρεί την ασφάλεια του αρχείου και το απόρρητο της επεξεργασίας επιλέγοντας συνεργάτες με επαγγελματικά προσόντα, τεχνικές γνώσεις και προσωπική ακεραιότητα. Όταν η επεξεργασία ανατίθεται σε εξωτερικό συνεργάτη

του υπεύθυνου επεξεργασίας, η ανάθεση γίνεται υποχρεωτικά εγγράφως και οι υποχρεώσεις τήρησης του Νόμου βαρύνουν αναλόγως και αυτόν (άρθρο 10, § 1-3).

Σύμφωνα με τα παραπάνω, η λειτουργία ενός πληροφοριακού συστήματος υγείας συνιστά σύσταση αρχείου, επεξεργασία δεδομένων προσωπικού χαρακτήρα, ειδικότερα, επεξεργασία ευαίσθητων δεδομένων και κατά συνέπεια περιορίζεται από τις παρακάτω διατάξεις.

Ο Νόμος επιτρέπει τη συλλογή και την επεξεργασία ευαίσθητων δεδομένων, καθώς και την ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής, εφόσον η επεξεργασία αφορά δεδομένα 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 όπως και για επιστημονικούς ή ερευνητικούς αποκλειστικά σκοπούς με την προϋπόθεση να τηρείται η ανωνυμία και να λαμβάνονται όλα τα απαραίτητα μέτρα για τη διαφύλαξη των δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα (άρθρο 7, § 2.δ' και 2.στ').

Συνεπώς, για την έναρξη λειτουργίας ενός πληροφοριακού συστήματος υγείας ή συστήματος διαχείρισης ηλεκτρονικών φακέλων ασθενών, ο υπεύθυνος επεξεργασίας, οφείλει να αιτείται εγγράφως στην Αρχή για άδεια συλλογής και επεξεργασίας ευαίσθητων δεδομένων. Εξαιρέση αποτελεί η επεξεργασία δεδομένων υγείας όταν γίνεται από ιατρούς ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από το ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει νόμος ή κώδικας δεοντολογίας, με την προϋπόθεση τα δεδομένα να μη διαβιβάζονται ή κοινοποιούνται σε τρίτους. Δεν εξαιρούνται όμως τα νομικά πρόσωπα ή οι οργανισμοί που παρέχουν υπηρεσίες υγείας καθώς και οι υπεύθυνοι επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν η επεξεργασία γίνεται στα πλαίσια προγραμμάτων τηλεϊατρικής ή παροχής ιατρικών υπηρεσιών μέσω δικτύου (άρθρο 7Α, § 8').

Επίσης, απαραίτητη προϋπόθεση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ευαίσθητων και μη, και την έγκριση της άδειας από την Αρχή, είναι η συλλογή τους με νόμιμα και θεμιτά μέσα, για καθορισμένους, σαφείς και νόμιμους σκοπούς. Η επεξεργασία των δεδομένων αυτών πρέπει να λαμβάνει χώρα μόνο για τους σκοπούς αυτούς και για το χρονικό διάστημα που ορίζει η Αρχή. Τα δεδομένα πρέπει να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας του προσώπου στο οποίο αναφέρονται μόνο κατά τη διάρκεια του χρονικού διαστήματος αυτού εκτός και αν οριστεί διαφορετικά από την Αρχή για στατιστικούς ή επιστημονικούς λόγους και μόνο αν δε θίγονται τα δικαιώματα των υποκειμένων

τους ή και τρίτων. Ακόμα, τα δεδομένα οφείλουν να είναι ακριβή και, εφόσον χρειάζεται, να ενημερώνονται, να είναι συναφή και όχι περισσότερα από όσα κάθε φορά απαιτείται για την επίτευξη του σκοπού για τον οποίο συλλέχθηκαν (άρθρο 4, § 1). Επιπλέον, η επεξεργασία επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του, εκτός αν συντρέχουν άλλοι νόμιμοι λόγοι, όπως, για παράδειγμα, η εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο (άρθρο 5, § 1 και 2). Στην κατηγορία αυτή εμπίπτουν και οι ιατροί, οι οποίοι υποχρεούνται από το άρθρο 14 του Ν.3418/2005 (Κώδικας Ιατρικής Δεοντολογίας) να τηρούν αρχείο (βλ. § 3.2.3).

Για τη χορήγηση άδειας η Αρχή μπορεί να επιβάλλει όρους και προϋποθέσεις έτσι ώστε να διασφαλιστεί αποτελεσματικά το δικαίωμα ιδιωτικής ζωής (άρθρο 7, § 3). Ως αίτηση για την απόκτηση άδειας θεωρείται η έγγραφη γνωστοποίηση του αρχείου ευαίσθητων δεδομένων από τον υπεύθυνο επεξεργασίας δηλώνοντας, μεταξύ άλλων, το σκοπό της επεξεργασίας των δεδομένων που περιέχονται ή πρόκειται να συμπεριληφθούν στο αρχείο, το είδος των δεδομένων που πρόκειται να υποστούν ή υφίστανται επεξεργασία ή πρόκειται να συμπεριληφθούν ή συμπεριλαμβάνονται στο αρχείο, το χρονικό διάστημα για το οποίο προτίθεται να εκτελεί την επεξεργασία ή να διατηρεί το αρχείο, τους αποδέκτες στους οποίους ενδέχεται να ανακοινώσει τα δεδομένα προσωπικού χαρακτήρα, τις ενδεχόμενες διαβιβάσεις και το σκοπό της διαβίβασης προσωπικών δεδομένων σε τρίτες χώρες και τέλος, τα βασικά χαρακτηριστικά του συστήματος και των μέτρων ασφαλείας του αρχείου ή της επεξεργασίας (άρθρο 6, § γ'-η').

Η τελευταία υποχρέωση του υπεύθυνου επεξεργασίας είναι πολύ σημαντική για την υλοποίηση πληροφοριακών συστημάτων υγείας και συστημάτων διαχείρισης ηλεκτρονικών φακέλων ασθενών καθώς προϋποθέτει τη μελέτη και εφαρμογή πολιτικής ασφάλειας στα συστήματα αυτά. Δεν είναι δυνατή η χορήγηση άδειας για επεξεργασία ευαίσθητων δεδομένων, όπως είναι τα δεδομένα υγείας, χωρίς πρώτα να υλοποιηθεί ένα σύστημα με την απαιτούμενη ασφάλεια για την προστασία των δεδομένων αυτών.

Η έννοια της ασφάλειας απασχολεί τον Έλληνα νομοθέτη και όσον αφορά τη διασυνοριακή ροή των δεδομένων. Συγκεκριμένα, η διαβίβαση των δεδομένων επιτρέπεται προς τις χώρες μη μέλη της Ευρωπαϊκής Ένωσης, κατόπιν άδειας της Αρχής, εφόσον η εν λόγω χώρα παρέχει ικανοποιητικό επίπεδο ασφάλειας όπως αυτό ορίζεται στην παράγραφο 2 του άρθρου 25 της Οδηγίας 95/46/ΕΚ. Η άδεια για τη διαβίβαση των δεδομένων χορηγείται λαμβάνοντας υπόψη, μεταξύ άλλων, τη φύση των δεδομένων, τα μέτρα ασφαλείας για την προστασία τους και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού. Αξίζει να

σημειωθεί πως διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα επιτρέπεται ελεύθερα σε χώρες-μέλη της Ευρωπαϊκής Ένωσης ενώ σε χώρες μη μέλη, δεν εξασφαλίζεται ικανοποιητικό επίπεδο προστασίας, επιτρέπεται, κατόπιν άδειας της Αρχής, υπό προϋποθέσεις (άρθρο 9, § 1-2).

Πριν τη δημιουργία αρχείου, και συνεπώς πριν τη λειτουργία του πληροφοριακού συστήματος υγείας, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο των δεδομένων με σαφή τρόπο για το σκοπό της επεξεργασίας, τους αποδέκτες των δεδομένων καθώς και του δικαιώματος πρόσβασης σε αυτά (άρθρο 11, § 1). Σε περίπτωση που τα δεδομένα ανακοινώνονται σε τρίτους, το πρόσωπο το οποίο αυτά αφορούν ενημερώνεται για την ανακοίνωση πριν από αυτούς (άρθρο 11, § 3). Επίσης, το υποκείμενο των δεδομένων έχει δικαίωμα να γνωρίζει αν δεδομένα προσωπικού χαρακτήρα που τον αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Ειδικότερα, όταν πρόκειται για δεδομένα υγείας, η γνωστοποίηση αυτών γίνεται από ιατρό (άρθρο 12, § 1 και 6). Τέλος, το υποκείμενο έχει το δικαίωμα να εκφράσει τις αντιρρήσεις του για την επεξεργασία των δεδομένων τα οποία των αφορούν με έγγραφη αίτηση προς τον υπεύθυνο επεξεργασίας (άρθρο 13, § 1).

Ο Νόμος 2472/1997 αποτελεί μια ακριβή μεταφορά της Οδηγίας 95/46/EK και αποτελεί τη ραχοκοκαλιά της ελληνικής νομοθεσίας όσον αφορά στην προστασία των δεδομένων προσωπικού χαρακτήρα. Στην ελληνική νομοθεσία δε συμπεριλαμβανόταν κάποιος νόμος σχετικά με την προστασία των προσωπικών δεδομένων. Η ψήφιση του Ν. 2472/1997 παρέχει τις βασικές αρχές προς αυτή την κατεύθυνση αλλά εξαιτίας του εύρους των δραστηριοτήτων στις οποίες αναφέρεται και τις οποίες καθορίζει αλλά και της αλματώδους ανάπτυξης της τεχνολογίας, δεν παρέχει λεπτομερή και ακριβή προστασία. Για αυτό το λόγο η Αρχή χρησιμοποιώντας το Νόμο ως σημείο αναφοράς, εκδίδει κανονιστικές πράξεις κατά περίπτωση. Τα κενά του Ν. 2472/1997, όσον αφορά στον τομέα των ηλεκτρονικών επικοινωνιών, ήρθε να καλύψει ο Ν. 3471/2006.

3.3.1.2 Νόμος 3471/2006

Ο Ν.3471/2006 αποτελεί ενσωμάτωση της Οδηγίας 2002/58/EK (βλ. § 3.3.2) στην ελληνική νομοθεσία. Ψηφίστηκε στις 27/06/2006 και δημοσιεύτηκε στην Εφημερίδα της Κυβερνήσεως την επόμενη ημέρα.

Σκοπός τον Νόμου είναι η προστασία των θεμελιώδους δικαιώματος της ιδιωτικής ζωής, η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την

προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (άρθρο 1, δεύτερο εδάφιο). Επίσης, στο δεύτερο κεφάλαιο του Νόμου γίνεται η αναθεώρηση του Ν.2472/1997. Με την έναρξη ισχύος τον Ν. 3471/2006 καταργείται ο Ν. 2774/1999, ο οποίος αφορούσε στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα (άρθρο 17).

Ο Ν 3471/2006 ορίζει τις βασικές έννοιες όσον αφορά τις ηλεκτρονικές επικοινωνίες, ρυθμίζει τις υποχρεώσεις των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών και ορίζει τα δικαιώματα των χρηστών. Το πεδίο εφαρμογής τον Νόμου περιλαμβάνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα στις διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών, ενώ οι αντίστοιχες υπηρεσίες που δεν είναι διαθέσιμες στο κοινό, όπως τα ιδιωτικά δίκτυα, ρυθμίζονται από το νόμο 2472/1997 (άρθρο 3, § 1).

- Συνδρομητής: κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών για την παροχή των υπηρεσιών αυτών (άρθρο 2, § 1).
- Χρήστης: κάθε φυσικό ή νομικό πρόσωπο που χρησιμοποιεί τις παραπάνω υπηρεσίες, για προσωπικό ή επαγγελματικό σκοπό, χωρίς να είναι απαραίτητα συνδρομητής των υπηρεσιών αυτών (άρθρο 2, § 2).
- Δεδομένα κίνησης: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας ή της χρέωσής της. Σε αυτή την κατηγορία περιλαμβάνονται, μεταξύ άλλων, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού του συνδρομητή ή χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης της επικοινωνίας καθώς και το δίκτυο προέλευσης ή προορισμού της επικοινωνίας (άρθρο 2, § 3)
- Δεδομένα θέσης: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και υποδεικνύουν τη γεωγραφική θέση του τερματικού του χρήστη (άρθρο 2, § 4).
- Επικοινωνία: κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών στα πλαίσια μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Σε αυτή την κατηγορία δεν ανήκουν οι πληροφορίες που διακινούνται ως τμήμα ραδιοτηλεοπτικών υπηρεσιών, εκτός από τις περιπτώσεις κατά τις οποίες οι πληροφορίες αφορούν αναγνωρίσιμο συνδρομητή ή χρήστη που τις λαμβάνει (άρθρο 2, § 5).

- Υπηρεσία προστιθέμενης αξίας: κάθε υπηρεσία η οποία επιβάλλει την επεξεργασία δεδομένων κίνησης ή θέσης πέρα από αυτά που απαιτούνται για τη μετάδοση μιας επικοινωνίας και τη χρέωσή της (άρθρο 2, § 7).
- Δημόσιο δίκτυο επικοινωνιών: το δίκτυο ηλεκτρονικών επικοινωνιών το οποίο χρησιμοποιείται, εξ ολοκλήρου ή κυρίως, για την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών (άρθρο 2, §10).
- Υπηρεσίες ηλεκτρονικών επικοινωνιών: οι υπηρεσίες που παρέχονται με μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών. Σε αυτή την κατηγορία δεν ανήκουν οι υπηρεσίες παροχής ή ελέγχου περιεχομένου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και υπηρεσίες της Κοινωνίας της Πληροφορίας που δεν αφορούν, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών (άρθρο 2, § 9).

Σύμφωνα με τα παραπάνω, τα πληροφοριακά συστήματα υγείας και τα συστήματα διαχείρισης ηλεκτρονικών φακέλων ασθενών, τα οποία διασυνδέονται μέσω δημοσίου δικτύου ηλεκτρονικών επικοινωνιών, πρέπει να συμμορφώνονται με τις διατάξεις του Νόμου 3471/2006.

Το άρθρο 4 του Νόμου ορίζει πως, οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, προστατεύεται από το απόρρητο των επικοινωνιών (§1). Με την επιφύλαξη της διατήρησης του απορρήτου, επιτρέπεται η τεχνικής φύσεως αποθήκευση όταν είναι αναγκαία για τη διαβίβαση της επικοινωνίας (§ 4). Επίσης, ο φορέας οφείλει, στο βαθμό που αυτό είναι τεχνικώς εφικτό, να καθιστά τη χρήση ή πληρωμή των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικής επικοινωνίας ανωνύμως ή με ψευδώνυμο (άρθρο 5, § 7). Η άρση του απορρήτου επιτρέπεται μόνο υπό τις προϋποθέσεις και τις διαδικασίες οι οποίες προβλέπονται από το άρθρο 19 του Συντάγματος (άρθρο 4, § 1).

Επιπλέον, απαγορεύεται η παρακολούθηση ή η επιτήρηση των ηλεκτρονικών επικοινωνιών, εκτός αν ορίζεται διαφορετικά από το νόμο (άρθρο 4, § 2). Απαγορεύεται, ακόμα, η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών στο τερματικό του χρήστη ή για την απόκτηση πρόσβασης σε αυτό. Σε αυτή την περίπτωση ανήκουν τα “cookies”, τα οποία αποτελούν κρυφές πληροφορίες που ανταλλάσσονται μεταξύ του

τερματικού του χρήστη και ενός web server με σκοπό της διατήρηση κάποιων πληροφοριών σχετικά με τη σύνδεση, όπως π. χ αν ο χρήστης έχει επισκεφτεί στο παρελθόν κάποια συγκεκριμένη ιστοσελίδα. Τα “cookies” μπορούν να χρησιμοποιηθούν για την παρακολούθηση της δραστηριότητας του χρήστη στο Διαδίκτυο και ως εκ τούτου αποτελούν απειλή για το δικαίωμα της ιδιωτικότητας. Ο συνδρομητής ή ο χρήστης πρέπει να έχει το δικαίωμα να αρνηθεί την αποθήκευση των “cookies” στο τερματικό του. Το ίδιο ισχύει και στην περίπτωση κακόβουλου λογισμικού, όπως πχ. τα λογισμικά “spyware”. Εξαίρεση στην παραπάνω απαγόρευση αποτελεί η τεχνικής φύσης αποθήκευση ή πρόσβαση όταν σκοπός της είναι η διευκόλυνση ή η διενέργεια μιας επικοινωνίας μέσω δικτύου ή όταν είναι αναγκαία για την παροχή υπηρεσίας, την οποία έχει ζητήσει ρητά ο χρήστης ή συνδρομητής. Σε αυτή την περίπτωση ο χρήστης ή συνδρομητής πρέπει πρώτα να έχει ενημερωθεί, σύμφωνα με το άρθρο 11 του Ν. 2472/1997, και να έχει το δικαίωμα να αρνηθεί αυτή την επεξεργασία (άρθρο 4, § 5).

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο αν ο συνδρομητής ή ο χρήστης, μετά από ενημέρωσή του για το είδος των δεδομένων, το σκοπό και την έκταση της επεξεργασίας και τους πιθανούς αποδέκτες, συναινεί σε αυτή ή αν η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι ο συνδρομητής ή ο χρήστης ή για τη λήψη μέτρων κατά το προσυμβατικό στάδιο, μετά από αίτησή του (άρθρο 5 § 2). Ο πάροχος δημοσίου δικτύου δεν επιτρέπεται να χρησιμοποιεί τα προσωπικά δεδομένα, τα δεδομένα κίνησης ή θέσης ή να τα διαβιβάζει σε τρίτους για άλλους σκοπούς, εκτός αν ο συνδρομητής ή χρήστης έχει ρητά και ειδικά δώσει τη συγκατάθεσή του (άρθρο 5 § 4). Η συγκατάθεση αυτή, όπου απαιτείται, δίδεται εγγράφως ή με ηλεκτρονικά μέσα. Στην τελευταία περίπτωση, ο υπεύθυνος επεξεργασίας εξασφαλίζει ότι ο συνδρομητής ή χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωσή του, η οποία καταγράφεται με ασφαλή τρόπο, είναι ανά πάσα στιγμή προσβάσιμη στο χρήστη και μπορεί να ανακληθεί οποτεδήποτε (άρθρο 5, § 3).

Ιδιαίτερα για τα δεδομένα κίνησης, σε περίπτωση που διαβιβάζονται σε τρίτους, η συγκατάθεση απαιτείται να είναι έγγραφη. Επίσης, ο φορέας οφείλει να ενημερώσει τον συνδρομητή ή χρήστη, πριν τη χορήγηση της συγκατάθεσης, για τον τύπο των δεδομένων κίνησης που επεξεργάζονται και τη διάρκεια της επεξεργασίας αυτής. Αν τα δεδομένα κίνησης διαβιβάζονται σε άλλους φορείς παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών με μοναδικό σκοπό τη χρέωση των παρεχόμενων επικοινωνιών, οι φορείς αυτή δε λογίζονται ως τρίτοι, με τον όρο ο συνδρομητής ή χρήστης να ενημερωθεί

εγγράφως για την κατάρτιση της σύμβασης. Και σε αυτή την περίπτωση η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε. Αν ανακληθεί, η ανάκληση αυτή ανακοινώνεται και στους τρίτους με ευθύνη του υπεύθυνου επικοινωνίας. Ο φορέας απαγορεύεται να εξαρτά την παροχή υπηρεσιών προς το συνδρομητή από τη συγκατάθεση του τελευταίου στην επεξεργασία των δεδομένων κίνησης, για σκοπούς άλλους από εκείνους που εξυπηρετούν άμεσα την παροχή των υπηρεσιών ηλεκτρονικής επικοινωνίας (άρθρο 5, § 5). Δηλαδή, ο φορέας δε μπορεί να αρνηθεί να παρέχει υπηρεσίες ηλεκτρονικής επικοινωνίας, αν ο συνδρομητής αρνηθεί να επεξεργάζονται τα δεδομένα κίνησης που αφορούν αυτές τις υπηρεσίες, για σκοπούς διαφορετικούς από τη διαβίβαση ή τη διευκόλυνση της επικοινωνίας. Τέτοιοι σκοποί θα μπορούσαν να είναι έρευνες μάρκετινγκ ή, στην περίπτωση των πληροφοριακών συστημάτων υγείας, στατιστικές ή ερευνητικές μελέτες.

Τα δεδομένα κίνησης που αφορούν συνδρομητές ή χρήστες, τα οποία υποβάλλονται σε επεξεργασία, καταστρέφονται ή καθίστανται ανώνυμα με κατάλληλη κωδικοποίηση, με τη λήξη της επικοινωνίας ή και μετά το πέρας αυτής, εφόσον είναι αναγκαίο για τη χρέωση των συνδρομητών, μετά από ενημέρωση από το φορέα παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών. Η επεξεργασία αυτή επιτρέπεται μόνο έως το τέλος της περιόδου εντός της οποίας μπορεί να αμφισβητηθεί νομίμως ο λογαριασμός ή να επιδιωχθεί η πληρωμή του (άρθρο 6, § 1-2).

Όσον αφορά τα δεδομένα θέσης, τα οποία αφορούν συνδρομητές ή χρήστες, επιτρέπεται η επεξεργασία τους για την παροχή υπηρεσίας προστιθέμενης αξίας, μόνον εφόσον αυτά καθίστανται ανώνυμα με την κατάλληλη κωδικοποίηση ή με τη ρητή συγκατάθεση του συνδρομητή ή χρήστη μετά από σχετική ενημέρωση του φορέα. Η συγκατάθεση αυτή μπορεί να ανακληθεί οποτεδήποτε. Στο συνδρομητή ή χρήστη πρέπει να παρέχεται η δυνατότητα, σε κάθε σύνδεση με το δίκτυο ή μετάδοση μιας επικοινωνίας, να αρνείται προσωρινά την επεξεργασία των δεδομένων αυτών, με απλά μέσα και ατελώς (άρθρο 6, § 3). Κατ' εξαίρεση, επιτρέπεται χωρίς προηγούμενη συγκατάθεση του συνδρομητή ή χρήστη, η επεξεργασία των εν λόγω δεδομένων προκειμένου να παρέχουν στις αρμόδιες αρχές για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης δεδομένα για τον εντοπισμό του καλούντος και μόνο για αυτό το σκοπό (άρθρο 6, § 4) 1 Περίπτωση έκτακτης ανάγκης μπορεί να είναι, για παράδειγμα, η κλήση στο τηλεφωνικό κέντρο του ΕΚΑΒ (Εθνικό Κέντρο Άμεσης Βοήθειας) για την αναφορά ατυχήματος ή έκτακτου περιστατικού.

Ιδιαίτερα για τις τηλεφωνικές κλήσεις, ο Νόμος ορίζει πως ο καλών χρήστης ή συνδρομητής πρέπει, εφόσον το επιθυμεί, να έχει τη δυνατότητα να αποκρύψει τον τηλεφωνικό του αριθμό, με απλά μέσα και ατελώς (άρθρο 8, § Ι). Η παραπάνω δυνατότητα του χρήστη ή συνδρομητή είναι πολύ σημαντική στις περιπτώσεις παροχής συμβουλών υγείας μέσω τηλεφώνου, όπου είναι επιθυμητή η ανωνυμία του καλούντα (Παρατηρητήριο για την Κοινωνία της Πληροφορίας, 2007:101). Παρόλα αυτά, ο φορέας οφείλει να διαθέτει μέσα εξουδετέρωσης της δυνατότητας μη αναγραφής της καλούσας γραμμής στην περίπτωση, μεταξύ άλλων, κλήσεων έκτακτης ανάγκης έτσι ώστε να δίδεται απάντηση στις κλήσεις αυτές ανεξάρτητα από την ύπαρξη προσωρινής συγκατάθεσης του συνδρομητή ή χρήστη. Τα δεδομένα που περιέχουν την αναγνώριση της ταυτότητας του καλούντος αποθηκεύονται και είναι διαθέσιμα από τη δημόσια υπηρεσία ή τον ιδιωτικό φορέα άμεσης επέμβασης, που έχει καλέσει ο συνδρομητής ή χρήστης, μόνο για το σκοπό της άμεσης απάντησης και επέμβασης και μόνο για το χρονικό διάστημα που είναι αναγκαίο για την επίτευξη του σκοπού αυτού, και στη συνέχεια διαγράφονται (άρθρο 8, § 7β').

Γενικότερα, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την επίτευξη των σκοπών της (άρθρο 5, § 1). Προς αυτή την κατεύθυνση πρέπει να γίνεται ο σχεδιασμός και η επιλογή των τεχνικών μέσων, των πληροφοριακών συστημάτων και του εξοπλισμού για την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών (άρθρο 5, § 6).

Με τις παραπάνω διατάξεις προστατεύεται το απόρρητο των πληροφοριών που μεταδίδονται μέσω ενός δημοσίου δικτύου ηλεκτρονικών επικοινωνιών. Συνεπώς, ένα πληροφοριακό σύστημα υγείας που προσφέρει υπηρεσίες, όπως τηλεφωνικά ραντεβού, ιστοσελίδα παροχής ιατρικών συμβουλών ή και τηλεφωνικό κέντρο άμεσης βοήθειας δεσμεύεται να προστατεύει την ιδιωτικότητα των χρηστών και το απόρρητο των πληροφοριών που ανταλλάσσονται. Η ιδιωτικότητα των χρηστών στις παραπάνω υπηρεσίες μπορεί να διαφυλαχτεί, για παράδειγμα, με τη χρήση ψευδωνύμων για την είσοδο στην ιστοσελίδα παροχής ιατρικών συμβουλών, τη χρήση κωδικού ανά ασθενή για τα ραντεβού με τους ιατρούς και, όπως ο Νόμος προβλέπει, μη αναγραφή του αριθμού του καλούντος.

Ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα, προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του καθώς και η ασφάλεια του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών. Τα μέτρα αυτά, εφόσον είναι αναγκαία, πρέπει να λαμβάνονται

από κοινού με τον πάροχο του δημοσίου δικτύου και να εγγυώνται επίπεδο ασφάλειας ανάλογο προς τον υπάρχοντα κίνδυνο, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες καθώς και του κόστους εφαρμογής τους (άρθρο 12, § 1). Αν υπάρχει ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δημοσίου δικτύου, ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να ενημερώνει τους συνδρομητές. Αν ο κίνδυνος αυτός είναι εκτός του πεδίου των μέτρων που οφείλει να λαμβάνει, πρέπει επιπλέον να ενημερώνει τους συνδρομητές για όλες τις δυνατότητες αποτροπής του κινδύνου και το κόστος αυτών (άρθρο 12, § 2). Επίσης, είναι ευθύνη του φορέα να αναθέτει την επεξεργασία δεδομένων προσωπικού χαρακτήρα και των συναφών δεδομένων κίνησης και θέσης, σε άτομα με τεχνική κατάρτιση και η επεξεργασία αυτή να περιορίζεται σε ενέργειες οι οποίες είναι απολύτως απαραίτητες για την εξυπηρέτηση σκοπών, όπως η διαχείριση των χρεώσεων ή της κίνησης, οι απαντήσεις σε ερωτήσεις των πελατών και άλλοι.

Συνεπώς, στην περίπτωση που τα πληροφοριακά συστήματα υγείας προσφέρουν υπηρεσίες ηλεκτρονικής επικοινωνίας σε δημόσιο δίκτυο επικοινωνιών, τόσο οι φορείς παροχής του δημοσίου δικτύου, όσο και οι φορείς παροχής υπηρεσιών υγείας, οφείλουν να λάβουν όλα τα απαραίτητα μέτρα ασφάλειας για την προστασία των δεδομένων που διακινούνται στο δίκτυο καθώς και τη διαφύλαξη του απορρήτου της επικοινωνίας.

Ο Ν. 3471/2006 αποτελεί ακριβή μεταφορά της Οδηγίας 2002/58/ΕΚ. Οι διατάξεις του προσφέρουν ευελιξία όσον αφορά στην τεχνική υλοποίηση των συστημάτων τα οποία προσφέρουν υπηρεσίες μέσω ενός δημοσίου δικτύου ηλεκτρονικών επικοινωνιών, όπως ορισμένα πληροφοριακά συστήματα υγείας, ενώ παράλληλα καθορίζουν τις υποχρεώσεις των φορέων παροχής των αντίστοιχων υπηρεσιών και δικτύων καθώς και τα δικαιώματα των συνδρομητών.

3.3.1.3 Νόμος 3418/2005

Ο Ν. 3418/2005 θεωρήθηκε στις 28/11/2005 και αντικατέστησε το Β Δ. της 25.5/6.7 1955 "Κανονισμός Ιατρικής Δεοντολογίας" (ΦΕΚ 171 Α'). Στο Ν. 3418/2005 διευκρινίζονται τα καθήκοντα και οι υποχρεώσεις των ιατρών κατά την άσκηση του επαγγέλματος τους, ορίζονται οι σχέσεις ιατρού και ασθενή καθώς και άλλες σημαντικές παράμετροι για την παροχή ιατρικής φροντίδας. Οι διατάξεις του Νόμου εφαρμόζονται κατά την άσκηση του ιατρικού επαγγέλματος και την παροχή υπηρεσιών υγείας, όπως αναφέρεται στο άρθρο 1, παράγραφος 5.

Όσον αφορά τα πληροφοριακά συστήματα και τα συστήματα διαχείρισης ηλεκτρονικών φακέλων ασθενών, ιδιαίτερο ενδιαφέρον παρουσιάζουν οι διατάξεις των άρθρων 13 και 14, οι οποίες αναφέρονται στο ιατρικό απόρρητο και την υποχρέωση τήρησης ιατρικού αρχείου αντιστοίχως.

Πιο συγκεκριμένα, στο άρθρο 13 δηλώνεται η υποχρέωση του ιατρού να τηρεί απόλυτη εχεμύθεια για οποιοδήποτε στοιχείο υποπέσει στην αντίληψή του ή του αποκαλύψει ο ασθενής ή τρίτοι, στο πλαίσιο άσκησης των καθηκόντων του, και αφορά στον ασθενή ή τους οικείους του, ακόμα και μετά το θάνατο του ασθενή (άρθρο 13, § 1 και 6). Δε δεσμεύονται με το ιατρικό απόρρητο, μόνο έναντι των εντολέων τους και μόνο ως προς το αντικείμενο της εντολής, οι ιατροί που ασκούν δημόσια υπηρεσία ελέγχου, επιθεώρησης ή πραγματογνωμοσύνης (άρθρο 13, § 5).

Σε αυτό το σημείο, είναι σημαντική η διαφοροποίηση του Ν.2472/1997 από τον Κώδικα Ιατρικής Δεοντολογίας όσον αφορά την υποχρέωση απορρήτου. Ο Ν.2472/1997 αναφέρεται μόνο σε ζώντα πρόσωπα, τα οποία είναι σε θέση να ασκήσουν τα δικαιώματα που ορίζονται στις διατάξεις του ενώ στο Ν. 3418/2005 η υποχρέωση απορρήτου επεκτείνεται και μετά το θάνατο του ασθενή (Μήτρου, 2006:25).

Η υποχρέωση τήρησης απορρήτου αναιρείται όταν ο ιατρός αποβλέπει στην εκπλήρωση νομικού καθήκοντος, όπως, για παράδειγμα, στις περιπτώσεις γέννησης ή θανάτου ή στην περίπτωση στην οποία λάβει γνώση για τη μελέτη κακουργηματικών πράξεων. Επίσης, ο ιατρός δε δεσμεύεται από το ιατρικό απόρρητο όταν αυτός αποβλέπει στη διαφύλαξη έννομου ή άλλου ουσιώδους, δημοσίου συμφέροντος ή συμφέροντος του ιδίου ή κάποιου άλλου, το οποίο δε μπορεί να διαφυλαχθεί διαφορετικά ή όταν συντρέχει κατάσταση ανάγκης ή άμυνας. Τέλος, επιτρέπεται η άρση του ιατρικού απορρήτου, αν ο ασθενής συναινέσει στην άρση αυτού σχετικά με τα δεδομένα που τον αφορούν, εφόσον η συναίνεση γίνεται με τρόπο θεμιτό και νόμιμο και η άρση του απορρήτου δε συνιστά προσβολή της ανθρώπινης αξιοπρέπειας (άρθρο 13, § 3-4).

Στο άρθρο 14 ορίζεται η υποχρέωση του ιατρού να τηρεί ιατρικό αρχείο, σε ηλεκτρονική ή μη μορφή, το οποίο περιέχει δεδομένα που συνδέονται αρρήκτως ή αιτιωδώς με την ασθένεια ή την υγεία των ασθενών του (άρθρο 14, § 1). Τα αρχεία αυτά πρέπει να περιέχουν το ονοματεπώνυμο, το πατρώνυμο, το φύλο, την ηλικία, το επάγγελμα, τη διεύθυνση του ασθενή, τις ημερομηνίες της επίσκεψης και κάθε άλλο ουσιώδες στοιχείο που συνδέεται με την παροχή ιατρικής φροντίδας στον ασθενή, όπως τα ενοχλήματα της υγείας του (άρθρο 14, § 2). Στο σημείο αυτό, ο ιατρός παραπέμπεται στο Ν. 2471/1997 για τους κανόνες τήρησης και

επεξεργασίας του αρχείου. Υποχρεούνται, επίσης, τα νοσοκομεία και οι κλινικές να τηρούν ιατρικό αρχείο καθώς και τα αποτελέσματα όλων των κλινικών και παρακλινικών εξετάσεων (άρθρο 14, § 2). Η υποχρέωση διατήρησης των αρχείων ισχύει για μια εικοσαετία από την τελευταία επίσκεψη του ασθενή, με εξαίρεση αυτή των ιδιωτικών ιατρείων, όπου η υποχρέωση ισχύει για μία δεκαετία (άρθρο 14, § 4).

Ο ιατρός υποχρεούται να διατηρεί τα επαγγελματικά του αρχεία με τέτοιον τρόπο, ώστε να εξασφαλίζεται το ιατρικό απόρρητο και η προστασία των προσωπικών δεδομένων ακόμα και μετά τη λήξη ή παύση του λειτουργήματος του (άρθρο 13, § 2β). Στα αρχεία αυτά επιτρέπονται μόνο κρίσεις ή σχολιασμοί που αφορούν στην ασθένεια των ασθενών και όχι προσωπικά σχόλια. Δικαίωμα πρόσβασης στα ιατρικά αρχεία έχει μόνο ο ασθενής στον οποίο αναφέρονται τα δεδομένα, ο οποίος μπορεί, επίσης, να αποκτήσει και αντίγραφο του φακέλου του. Εξαίρεση αποτελούν οι συγγενείς του ασθενή μέχρι τετάρτου βαθμού, μετά το θάνατο αυτού, οι δικαστικές και εισαγγελικές αρχές κατά την άσκηση των καθηκόντων τους ή άλλα όργανα της Ελληνικής Πολιτείας, που βάσει των καταστατικών τους διατάξεων έχουν τέτοιο δικαίωμα (άρθρο 14, § 8-9).

3.3.2 Ευρωπαϊκή Ένωση

Σε ευρωπαϊκό επίπεδο, το δικαίωμα της ιδιωτικότητας και το δικαίωμα της προστασίας των δεδομένων προσωπικού χαρακτήρα κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, αντίστοιχα. Πιο συγκεκριμένα, το άρθρο 7 ορίζει πως “κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του 37 ενώ το άρθρο 8 ορίζει, μεταξύ άλλων, πως “κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν”.

Το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο σε μια προσπάθεια εξίσωσης του επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα και διασφάλισης της ομαλής λειτουργίας της εσωτερικής αγοράς ανάμεσα στα μέλη της Κοινότητας, εξέδωσε την Οδηγία 95/46/EK. Στη συνέχεια, οι εξελίξεις στην τεχνολογία, ιδιαίτερα στον τομέα των ηλεκτρονικών επικοινωνιών, οδήγησαν αρχικά στην έκδοση της Οδηγίας 97/66/EK και έπειτα στην έκδοση της Οδηγίας 2002/58/EK.

3.3.2.1 Οδηγία 95/46/ΕΚ

Για την πρόσταζα των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης υπογράφηκε στις 24/10/1995. Στόχος αυτής είναι η προστασία θεμελιωδών ελευθεριών και δικαιωμάτων των φυσικών προσώπων, ιδίως της ιδιωτικής ζωής, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και η ελεύθερη κυκλοφορία των δεδομένων αυτών μεταξύ των κρατών-μελών». Τα κράτη- μέλη όφειλαν να εντάξουν την Οδηγία στο εθνικό τους δίκαιο εντός τριών ετών από την έκδοσή της (άρθρο 32, § 1). Η Ελλάδα ενσωμάτωσε την Οδηγία με το Ν. 2472/1997.

Στην Οδηγία γίνεται ο ορισμός των βασικών εννοιών που αφορούν στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθορίζεται το πλαίσιο της επεξεργασίας τους καθώς και η διασυννοριακή ροή των δεδομένων αυτών μεταξύ των κρατών-μελών. Επίσης, δίνονται οδηγίες για τη συγκρότηση μιας ανεξάρτητης αρχής, η οποία επιφορτίζεται με το έργο του ελέγχου της εφαρμογής των εθνικών διατάξεων, που αφορούν στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και της συμμόρφωσης αυτών με την Οδηγία (άρθρο 28).

Επίσης, η Οδηγία ορίζει τη σύσταση μιας ανεξάρτητης ομάδας, με συμβουλευτικό χαρακτήρα, για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (Ομάδα). Η Ομάδα απαρτίζεται από έναν αντιπρόσωπο της Αρχής κάθε κράτους-μέλους καθώς και έναν αντιπρόσωπο της Ευρωπαϊκής Επιτροπής (άρθρο 29, § 1 -2) και έχει ως αποστολή να εξετάζει κάθε θέμα σχετικό με την εφαρμογή των εθνικών διατάξεων σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα για να επιτύχει την ομοιόμορφη εφαρμογή τους. Επίσης, η Ομάδα παρέχει τη γνώμη της στην Ευρωπαϊκή Επιτροπή σχετικά με το επίπεδο προστασίας των κρατών-μελών και των τρίτων χωρών και συμβουλεύει την Επιτροπή για κάθε σχέδιο τροποποίησης της Οδηγίας ή συμπληρωματικών μέτρων που πρέπει να ληφθούν για την προστασία των δεδομένων προσωπικού χαρακτήρα (άρθρο 30, § 1).

Οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα μεταφέρθηκαν επακριβώς στο ελληνικό δίκαιο με το Ν. 2472/1997. Συνεπώς, τα δεδομένα προσωπικού χαρακτήρα διαχωρίζονται σε ευαίσθητα και μη ευαίσθητα (άρθρο 2, § α'-β'), η νομιμότητα της επεξεργασίας τους εξαρτάται, μεταξύ άλλων, από τη συγκατάθεση του υποκειμένου των δεδομένων (άρθρο 7, § α') ενώ η επεξεργασία ευαίσθητων δεδομένων που

αφορούν στην υγεία επιτρέπεται, εφόσον είναι αναγκαία για την ιατρική πρόληψη ή διάγνωση ή τη διαχείριση ιατροφαρμακευτικών υπηρεσιών και την παροχή ιατροφαρμακευτικής αγωγής, με την προϋπόθεση η επεξεργασία να γίνεται από πρόσωπο το οποίο δεσμεύεται από το ιατρικό απόρρητο ή αντίστοιχη υποχρέωση (άρθρο 8, § 3).

Όσον αφορά στη διασυνοριακή ροή δεδομένων, επιτρέπεται εφόσον η χώρα προορισμού των δεδομένων εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Το επίπεδο αυτό σταθμίζεται λαμβανομένων υπόψη όλων των περιστάσεων που επηρεάζουν τη διαβίβαση των δεδομένων. Η Ευρωπαϊκή Επιτροπή και τα κράτη-μέλη ενημερώνονται αμοιβαία αν θεωρούν ότι μία χώρα δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας και λαμβάνουν μέτρα για την αποφυγή οποιασδήποτε διαβίβασης δεδομένων προσωπικού χαρακτήρα προς τη χώρα αυτή (άρθρο 25, § 1-4). Κατ' εξαίρεση των παραπάνω, είναι δυνατόν να επιτραπεί η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς μια τρίτη χώρα εφόσον, και όχι περιοριστικά, το υποκείμενο των δεδομένων έχει συναινέσει ρητώς στη διαβίβαση, ή η διαβίβαση αυτή είναι αναγκαία για την εκτέλεση σύμβασης προς το συμφέρον του υποκειμένου ή πραγματοποιείται από δημόσιο μητρώο, το οποίο προορίζεται βάσει νομοθετικών ή άλλων διατάξεων για την παροχή πληροφοριών στο κοινό (άρθρο 26, § 1).

Η προτροπή προς τα κράτη-μέλη να ενθαρρύνουν την εκπόνηση κωδίκων δεοντολογίας για την προστασία των δεδομένων προσωπικού χαρακτήρα, οι οποίοι υποβάλλονται προς εξέταση στην εθνική Αρχή και την Ομάδα (άρθρο 27, § 1-2), υλοποιήθηκε στην Ελλάδα με την κατάργηση του Β.Δ. της 25.5/6.7.1955 "Κανονισμός Ιατρικής Δεοντολογίας" (ΦΕΚ 171 Α') και της ψήφισης του Ν.3418/2005.

3.3.2.2 Οδηγία 2002/58/ΕΚ

Οδηγία σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες). Η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης υπογράφηκε στις 12/07/2002 και τα κράτη-μέλη είχαν υποχρέωση να συμμορφωθούν έως τις 31/10/2003 (άρθρο 17, § 1).

Στόχος της είναι η εξειδίκευση και συμπλήρωση της Οδηγίας 95/46/ΕΚ για την προστασία της ιδιωτικής ζωής των φυσικών και νομικών προσώπων στις ηλεκτρονικές επικοινωνίες και η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα, των

εξοπλισμών και των υπηρεσιών ηλεκτρονικών επικοινωνιών ανάμεσα στα κράτη-μέλη (άρθρο 1, § 1-2). Η Οδηγία 2002/58/EK, σε αντίθεση με την Οδηγία 95/46/EK, παρέχει προστασία και στους συνδρομητές που είναι νομικά πρόσωπα και εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στα πλαίσια της παροχής διαθέσιμων στο κοινό υπηρεσιών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικής επικοινωνίας (άρθρο 3, § 1). Με την εφαρμογή της καταργείται η Οδηγία 97/66/EK (άρθρο 19), Η Οδηγία ενσωματώθηκε, εκπρόθεσμα, στο ελληνικό δίκαιο με το Ν.3471/2006.

Στην Οδηγία 2002/58/EK δίνονται οι βασικοί ορισμοί των χρηστών, της επικοινωνίας, της κλήσης, του ηλεκτρονικού ταχυδρομείου, των υπηρεσιών προστιθέμενης αξίας και των δεδομένων κίνησης και θέσης σε ένα δημόσιο δίκτυο ηλεκτρονικών επικοινωνιών (άρθρο 2, § α'-ε', ζ'-η'). Οι ορισμοί αυτοί μεταφέρθηκαν στο Ν.3472/2006 με ακρίβεια. Επίσης, γίνεται αναφορά στη συγκατάθεση του υποκειμένου, όπως αυτή ορίζεται στην Οδηγία 95/46/EK (άρθρο 2, § στ').

Η ασφάλεια των παρεχόμενων υπηρεσιών είναι ευθύνη του φορέα παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών, ο οποίος καλείται να συνεργαστεί, αν αυτό είναι αναγκαίο, με το φορέα παροχής του δημοσίου δικτύου, προκειμένου να κατοχυρώσει επίπεδο ασφάλειας ανάλογο με τον υπάρχοντα κίνδυνο, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες και το κόστος αυτών (άρθρο 4, § 1). Στην περίπτωση που υπάρχει ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δικτύου, ο φορέας οφείλει να ενημερώσει τους συνδρομητές για τον κίνδυνο αυτό, για τα μέτρα που μπορούν να λάβουν για την αποτροπή του και το κόστος αυτών, εφόσον ο κίνδυνος είναι πέρα των μέτρων που ο φορέας είναι υποχρεωμένος να λαμβάνει (άρθρο 4, § 2).

Οι ρυθμίσεις που ορίζονται στο άρθρο 5 σχετικά με το απόρρητο των επικοινωνιών και των συναφών δεδομένων κίνησης, εφαρμόστηκαν με ακρίβεια στο Ν 3471/2006. Συνεπώς, προστατεύεται το απόρρητο των επικοινωνιών, εκτός αν ορίζεται διαφορετικά από το Νόμο (άρθρο 5, § 1), όπως π.χ. στην περίπτωση της δίωξης ποινικών αδικημάτων ή της διαφύλαξης της εθνικής ασφάλειας (άρθρο 15, § 1). Δεν επιτρέπεται η αποθήκευση πληροφοριών ή η πρόσβαση στο τερματικό του χρήστη, εκτός αν πρόκειται για τεχνικής φύσης αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή η διευκόλυνση της επικοινωνίας. Επίσης, είναι δυνατή η αποθήκευση ή η πρόσβαση στο τερματικό του χρήστη, εφόσον ο τελευταίος έχει ενημερωθεί όπως ορίζεται στην Οδηγία 95/46/EK και ο υπεύθυνος ελέγχου των δεδομένων του παρέχει το δικαίωμα να αρνείται την επεξεργασία αυτή.

Ειδικότερα, τα δεδομένα κίνησης τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον πάροχο δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, πρέπει να διαγράφονται ή να καθίστανται ανώνυμα μετά το πέρας της επικοινωνίας (άρθρο 6, § 1), εκτός αν αφορούν στη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων. Στην τελευταία περίπτωση η επεξεργασία των εν λόγω δεδομένων επιτρέπεται μόνον έως το τέλος της χρονικής περιόδου εντός της οποίας μπορεί νόμιμα να αμφισβητηθεί ο λογαριασμός ή να επιδιωχθεί η πληρωμή του (άρθρο 6, § 2). Ο φορέας παροχής υπηρεσιών οφείλει να ενημερώνει το συνδρομητή ή τον χρήστη σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία και τη διάρκεια της επεξεργασία αυτής (άρθρο 6, § 4). Η επεξεργασία των δεδομένων κίνησης πρέπει να περιορίζεται σε πρόσωπα τα οποία ενεργούν υπό την εποπτεία του φορέα παροχής του δικτύου ή της διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών και πρέπει να περιορίζεται στα απολύτως απαραίτητα για την εξυπηρέτηση, μεταξύ άλλων, των σκοπών της χρέωσης, της ανίχνευσης της απάτης ή την παροχή υπηρεσίας προστιθέμενης αξίας (άρθρο 6, § 5).

Τα παραπάνω ισχύουν και για τα δεδομένα θέσης, με τη διαφορά πως οι συνδρομητές ή χρήστες θα πρέπει να έχουν τη δυνατότητα, με απλά μέσα και ατελώς, να αρνούνται προσωρινά την επεξεργασία των δεδομένων θέσης που τους αφορούν για κάθε σύνδεση στο δίκτυο ή για κάθε μετάδοση μιας επικοινωνίας (άρθρο 9, § 2).

Η Οδηγία ορίζει επίσης πως τα κράτη-μέλη δε θα πρέπει να επιβάλλουν κάποια υποχρεωτική απαίτηση σχετικά με ειδικά τεχνικά χαρακτηριστικά στις τερματικές συσκευές ή στον άλλο εξοπλισμό ηλεκτρονικών επικοινωνιών, έτσι ώστε να μην παρακωλύεται η ελεύθερη κυκλοφορία του εξοπλισμού αυτού και η διάθεσή του στα κράτη-μέλη και μεταξύ αυτών (άρθρο 14, § 1). Σε περίπτωση που η εφαρμογή κάποιων διατάξεων μπορεί να επιτευχθεί μόνο βάσει ειδικών τεχνικών χαρακτηριστικών, τα κράτη-μέλη οφείλουν να ενημερώσουν σχετικά την Επιτροπή για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών (άρθρο 14, § 2).

Η Οδηγία 2002/58/EK τροποποιήθηκε από την Οδηγία 2006/24/EK έτσι ώστε να επιτρέπεται η διατήρηση συγκεκριμένων δεδομένων για την αναγνώριση των συνδρομητών ή των χρηστών, με σκοπό τη διάθεσή τους στις αρμόδιες εθνικές αρχές για τη διαλεύκανση σοβαρών ποινικών αδικημάτων. Τα δεδομένα, τα οποία διατηρούνται για χρονικό διάστημα μεγαλύτερο των έξι μηνών και μικρότερο των δύο ετών (Οδηγία 2006/24/EK άρθρο 6),

τυγχάνουν προστασίας , με ευθύνη του φορέα, όπως ορίζεται στις Οδηγίες 95/46/EK και 2002/58/EK.

3.3.2.3 Οδηγία 2006/24/EK

Οδηγία για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/EK.

Η Οδηγία 2006/24/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου υπογράφηκε από τα κράτη- μέλη στις 15/03/2006. Στόχος της Οδηγίας είναι η εναρμόνιση των διατάξεων των κρατών-μελών σχετικά με τις υποχρεώσεις των παρόχων διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών όσον αφορά τη διατήρηση ορισμένων δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία από αυτούς, ώστε να διασφαλιστεί ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης και δίωξης σοβαρών ποινικών αδικημάτων (άρθρο 1, § 1). Η Οδηγία εφαρμόζεται στα δεδομένα κίνησης και θέσης, στα φυσικά και νομικά πρόσωπα και στα συναφή δεδομένα που απαιτούνται για την αναγνώριση των συνδρομητών ή των χρηστών και όχι στο περιεχόμενο των ηλεκτρονικών επικοινωνιών (άρθρο 1, § 2). Επίσης, στο άρθρο 11 αναθεωρείται η Οδηγία 2002/58/EK.

Στην Οδηγία εισάγονται δύο νέοι ορισμοί, ο κωδικός ταυτότητας του χρήστη και ο κωδικός ταυτότητας της κυψέλης. Ως κωδικός ταυτότητας του χρήστη νοείται ο μοναδικός αναγνωριστικός κωδικός που αποδίδεται σε κάθε πρόσωπο που καθίσταται συνδρομητής ή εγγράφεται σε κάποια υπηρεσία πρόσβασης στο Διαδίκτυο ή επικοινωνίας μέσω Διαδικτύου. Ως κωδικός ταυτότητας της κυψέλης ορίζεται η ταυτότητα του κυψελωτού κυττάρου από το οποίο ξεκινά ή στο οποίο καταλήγει συγκεκριμένη κλήση κινητής τηλεφωνίας (άρθρο 2, § ε'- δ'). Οι κατηγορίες των δεδομένων που διατηρούνται είναι οι ακόλουθες:

Όσον αφορά στα δεδομένα τα οποία είναι αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας, διατηρούνται ο τηλεφωνικός αριθμός του καλούντος και το ονοματεπώνυμο και η διεύθυνση του συνδρομητή, στην περίπτωση της σταθερής ή κινητής τηλεφωνίας. Στην περίπτωση της πρόσβασης στο Διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω Διαδικτύου διατηρούνται ο κωδικός ταυτότητας του χρήστη, ο τηλεφωνικός αριθμός του, το ονοματεπώνυμο και η διεύθυνση του συνδρομητή (άρθρο 5, § Ιβ').

Για τον προσδιορισμό της ημερομηνίας, της ώρας και της διάρκειας της επικοινωνίας όσον αφορά την πρόσβαση στο Διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω Διαδικτύου, διατηρούνται η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με το Διαδίκτυο ή με την υπηρεσία ηλεκτρονικού ταχυδρομείου ή τηλεφωνίας μέσω Διαδικτύου, βάσει συγκεκριμένης ωριαίας ζώνης. Επίσης, διατηρούνται ο κωδικός ταυτότητας χρήστη του συνδρομητή και η IP που δόθηκε στην επικοινωνία από τον πάροχο. Στην περίπτωση της σταθερής και κινητής τηλεφωνίας αποθηκεύονται η ημερομηνία και η ώρα έναρξης και λήξης της επικοινωνίας (άρθρο 5, § 1γ). Όσον αφορά στον προσδιορισμό του εξοπλισμού επικοινωνίας ή του φερόμενου ως εξοπλισμού επικοινωνίας των χρηστών στην τηλεφωνία σταθερού δικτύου, διατηρούνται οι τηλεφωνικοί αριθμοί του καλούντος και του καλουμένου. Επιπλέον, στην κινητή τηλεφωνία αποθηκεύονται η IMSI και η IMEI του καλούντος και του καλουμένου. Εάν πρόκειται για προπληρωμένη, ανώνυμη υπηρεσία κινητής τηλεφωνίας διατηρούνται η ημερομηνία και ώρα της αρχικής ενεργό ποιήσης της υπηρεσίας αυτής και ο κωδικός ταυτότητας κυψέλης από την οποία πραγματοποιήθηκε η ενεργοποίηση. Για τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω Διαδικτύου και πρόσβασης στο Διαδίκτυο, αποθηκεύονται ο τηλεφωνικός αριθμός του καλούντος για την πρόσβαση μέσω τηλεφώνου ή η ψηφιακή συνδρομητική γραμμή (DSL) (άρθρο 5, § 1ε').

Για τον προσδιορισμό της θέσης του εξοπλισμού κινητής επικοινωνίας διατηρούνται ο κωδικός ταυτότητας κυψέλης κατά την έναρξη της επικοινωνίας και τα δεδομένα με τα οποία προσδιορίζεται η γεωγραφική θέση των κυψελών κατά τη διάρκεια του χρονικού διαστήματος για το οποίο διατηρούνται τα δεδομένα των επικοινωνιών (άρθρο 5, § 1στ').

Αξίζει να σημειωθεί πως δεν επιτρέπεται η διατήρηση δεδομένων που αποκαλύπτουν το περιεχόμενο των επικοινωνιών (άρθρο 5, § 2). Επιπλέον, πρέπει τα κράτη-μέλη να διασφαλίζουν ότι τα δεδομένα που διατηρούνται παρέχονται μόνο στις αρμόδιες αρχές σε ειδικές περιπτώσεις που ορίζονται από την εθνική νομοθεσία (άρθρο 4).

Τα κράτη-μέλη υποχρεούνταν να συμμορφωθούν με την Οδηγία έως τις 15/09/2007 (άρθρο 15, § 1). Η Ελλάδα, μεταξύ άλλων κρατών-μελών, έκανε χρήση της παραγράφου 3 του άρθρου 15, η οποία επιτρέπει στα κράτη-μέλη να καθυστερήσουν την εφαρμογή της Οδηγίας ως προς τη φύλαξη δεδομένων επικοινωνίας που αφορούν την πρόσβαση στο Διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω Διαδικτύου, αποφασίζοντας να αναβάλλει την εφαρμογή της Οδηγίας το αργότερο μέχρι τις 18/03/2009.

Συμπεράσματα

Ο παραδοσιακός φάκελος ασθενή περιέχει μια πληθώρα δεδομένων που, κατά κύριο λόγο, εισάγονται από γιατρούς και νοσηλευτές, αλλά και από άλλους επαγγελματίες υγείας ή διοικητικό προσωπικό. Εκτός από τις προσωπικές εκτιμήσεις των συγκεκριμένων χρηστών, στο φάκελο ασθενή εισάγονται τα αποτελέσματα των εργαστηριακών εξετάσεων, οι ακτινογραφίες, οι αξονικές τομογραφίες, τα υπερηχογραφήματα, τα ηλεκτροκαρδιογραφήματα, τα ηλεκτροεγκεφαλογραφήματα, τα αποτελέσματα βιοψιών και πλήθος άλλων πληροφοριών σχετικά με κάθε ασθενή. Αν εξαιρέσει κανείς κάποιες εξετάσεις, οι οποίες εμφανίζονται με τη μορφή διαγραμμάτων, και τις εικόνες, τα περισσότερα δεδομένα εμφανίζονται ως κείμενο ή αριθμοί. Τέλος, στα περισσότερα νοσοκομειακά ιδρύματα οι φάκελοι ασθενή είναι χειρόγραφοι, είτε εξ ολοκλήρου είτε στο μεγαλύτερο μέρος τους.

Ωστόσο, τα διαφαινόμενα οφέλη από τη διατήρηση των φακέλων σε ηλεκτρονική μορφή, μέσα από τη δημιουργία ισχυρών υπολογιστικών συστημάτων που υποστηρίζουν την αποθήκευση, διατήρηση και επεξεργασία των δεδομένων ασθενή, πιέζουν για τη μετάβαση από το χειρόγραφο φάκελο στον ηλεκτρονικό φάκελο ασθενή).

Ο ηλεκτρονικός φάκελος ασθενή μπορεί να προσφέρει αδιαμφισβήτητα οφέλη στη φροντίδα υγείας. Ο ασθενής αποκομίζει οφέλη από την άμεση προσπέλαση των δεδομένων του, την ταχεία παραγωγή εγγράφων που τον αφορούν, την υποστήριξη της απόφασης των επαγγελματιών υγείας, την αυτοματοποίηση πολλών διαδικασιών και τη διασύνδεση με τα λοιπά υποσυστήματα του χώρου της υγείας. Έμμεσα οφέλη προκύπτουν και από τη χρησιμοποίηση του ηλεκτρονικού φακέλου στην έρευνα και στην εκπαίδευση των επαγγελματιών υγείας. Ένα ακόμη σημαντικό ζήτημα είναι ο σχεδιασμός, η υλοποίηση και η διαλειτουργικότητα του συστήματος του φακέλου ασθενή με τα υπόλοιπα υποσυστήματα του ιδρύματος.

Επίσης, εξαιρετικής σημασίας είναι η δομημένη εισαγωγή δεδομένων στον ηλεκτρονικό φάκελο. Αυτό διασφαλίζεται, κυρίως, με την κατασκευή φιλικών συστημάτων διεπαφής και δυναμικά με συστήματα που επεξεργάζονται το ελεύθερο κείμενο ή τη φωνή του χρήστη. Η ετερογένεια των πηγών της πληροφορίας που πρόκειται να συμπεριληφθεί στο φάκελο καθιστά αναγκαία την ύπαρξη τέτοιων συστημάτων.

Σε όλα αυτά πρέπει να προστεθεί η ασφάλεια των προσωπικών δεδομένων του ασθενή και η διαφύλαξη του ιατρικού απόρρητου. Άλλωστε, το ζήτημα της ασφάλειας αποτελεί εμπόδιο για την ενσωμάτωση του ηλεκτρονικού φακέλου στις κάρτες δεδομένων των ασθενών. Ωστόσο, οι κάρτες δεδομένων μπορούν να κάνουν τον ηλεκτρονικό φάκελο πιο λειτουργικό και πιο ασφαλή αν χρησιμοποιηθούν με ανάλογο τρόπο. Στην κατεύθυνση της σωστής εφαρμογής συστημάτων ηλεκτρονικού φακέλου στοχεύουν διάφοροι διεθνείς οργανισμοί προτυποποίησης που προτείνουν κανόνες οι οποίοι διέπουν την αρχιτεκτονική και τις λειτουργίες αυτών των συστημάτων.

Προκειμένου όμως να επιτευχθούν τα παραπάνω χρειάζεται να υπάρξουν ορισμένες προϋποθέσεις. Η παρούσα εργασία εστιάζοντας κυρίως σε βασικά ερευνητικά ερωτήματα όπως:

- ο τρόπος λειτουργίας του ιατρικού φακέλου και τα συστατικά του,
- ο τρόπος που εισάγονται δεδομένα σε αυτόν και
- η ασφάλεια των δεδομένων του ΗΦΥ

και με σκοπό την διερεύνηση της μετάβασης από τον ιατρικό φάκελο στον ηλεκτρονικό ιατρικό φάκελο, τονίζοντας τα οφέλη που μπορεί αυτός να επιφέρει στην υγεία και στον ίδιο τον ασθενή, ανέδειξε κάποιες μελλοντικές προκλήσεις και δράσεις που θα βοηθήσουν στην αντιμετώπιση των εμποδίων προς υλοποίηση του συστήματος ΗΦΥ.

Η διατριβή αυτή ανέδειξε την ανάγκη για οργανωτική δομή ενός συστήματος υγείας και εξειδικευμένου προσωπικού σε θέματα διοίκησης και οργάνωσης υπηρεσιών υγείας και ότι σημαντικό ρόλο καλούνται να παίξουν όλοι οι εμπλεκόμενοι φορείς ιατρικό προσωπικό, διοικητικό προσωπικό και οι ιατρικές επιστημονικές εταιρείες. Πρέπει να δοθεί έμφαση στη μεγάλη δυσκολία για αποδοχή και ενσωμάτωση της πληροφορικής τεχνολογίας στα συστήματα υγείας, κυρίως στην αντίσταση του ιατρικού σώματος που είναι αρνητικό στη χρήση υπολογιστών. Να λυθούν προβλήματα που πηγάζουν από την έλλειψη βασικής πληροφόρησης και εκπαίδευσης και ενδεχομένως όχι από τη μη αποδοχή της τεχνολογίας, καθώς η αποδοχή ενός συστήματος ΗΦΥ είναι ένα θέμα νοοτροπίας και κουλτούρας. Η εφαρμογή ενός συστήματος ΗΦΥ θα πρέπει επίσης να στηρίζεται στη φιλικότητα προς τον τελικό χρήστη, γιατί η επιτυχία υλοποίησης ενός συστήματος ΗΦΥ, στο μεγαλύτερο βαθμό εξαρτάται από τον

ανθρώπινο παράγοντα και σε μικρότερο βαθμό από την τεχνολογία. Το θέμα του ηλεκτρονικού φακέλου δεν πρέπει να θεωρείται μόνο σαν τεχνολογικό ζήτημα αλλά και ως κοινωνικό.

Η ανάγκη τυποποίησης των δεδομένων που παράγουν οι φορείς υγείας γίνεται πιο έντονη, προκειμένου να γίνει πραγματικότητα η βελτίωση των υπηρεσιών υγείας με την ανάπτυξη σύγχρονων πληροφοριακών συστημάτων. Σημαντικό ανασταλτικό παράγοντα αποτελεί η μικρή ανάπτυξη προτύπων ιατρικής πληροφορικής καθώς και η χρήση διεθνών προτύπων κωδικοποίησης και διαλειτουργικότητας που επιτρέπουν τη χρήση της συσσωρευμένης, αξιόπιστης και κωδικοποιημένης πληροφορίας για δευτερογενή χρήση. Είναι απολύτως απαραίτητο να καλυφθεί το θέμα της τεχνικής διαλειτουργικότητας και της περιπλοκότητας των συστημάτων υγείας διευκολύνοντας έτσι την αναδιοργάνωση των συστημάτων και των ροών της πληροφορίας ανάμεσα στους άμεσα ενδιαφερόμενους, καθώς το θέμα αυτό αποτελεί απαραίτητη προϋπόθεση για την πρόοδο της τεχνολογίας με γνώμονα την καλύτερη εξυπηρέτηση του πολίτη και τη βελτίωση του βιοτικού επιπέδου του.

Επίσης στην διατριβή αυτή γίνεται εκτενής έκθεση όσο αφορά το θεσμικό και ρυθμιστικό πλαίσιο σχετικά με τη διαχείριση των ευαίσθητων και προσωπικών δεδομένων τονίζοντας το θέμα της προστασίας της ιδιωτικότητας. Η ιδιωτικότητα ως απαίτηση ασφάλειας σε ένα πληροφοριακό σύστημα υγείας περιλαμβάνει άλλες απαιτήσεις ασφάλειας όπως η εμπιστευτικότητα, η εξουσιοδότηση, η μη αποποίηση και η ανωνυμοποίηση. Κατά συνέπεια δημιουργείται η ανάγκη ενίσχυσης προστασίας των πληροφοριών και των δεδομένων που επεξεργάζονται τα πληροφοριακά συστήματα από νέες ισχυρότερες τεχνολογικές λύσεις (μηχανισμούς ασφάλειας ,κρυπτογραφικοί μηχανισμοί) από αυτές που προτάθηκαν στην εργασία αυτή, όπως για παράδειγμα οι Τεχνολογίες Προστασίας Της Ιδιωτικότητας (Privacy Enhancing Technologies - PETs).

Επίσης κάθε κράτος θα πρέπει να θεσπίσει το κατάλληλο νομικό πλαίσιο για τη δημιουργία ενός πετυχημένου συστήματος ηλεκτρονικού φακέλου υγείας το οποίο θα προβλέπει τα κατάλληλα μέτρα για την αποτροπή της υποκλοπής των προσωπικών δεδομένων υγείας του ασθενή και γενικά οποιασδήποτε παραβίαση της ιδιωτικότητας. Πρέπει να εξασφαλιστούν οι αναγκαίες νομικές εγγυήσεις σε συνδυασμό με τις τεχνολογικές εγγυήσεις για την ασφάλεια και προστασία των δεδομένων σε κάθε φάση της ανάπτυξης του συστήματος. Κάθε κυβέρνηση καλείται να θεσπίσει την κατάλληλη νομοθεσία , αναλαμβάνοντας έτσι τις ευθύνες της και εναρμονίζοντας την παρούσα νομοθεσία με την αναδυόμενη τεχνολογία καλύπτοντας τα διάφορα κενά που υπάρχουν

Η εργασία αυτή, λοιπόν, έρχεται να συμβάλει στο χώρο της Ηλεκτρονικής Υγείας και πιο συγκεκριμένα στον τομέα των Ηλεκτρονικών Φακέλων. Προσφέρει μια γενική επισκόπηση των κύριων όψεων της Πληροφορικής Υγείας, καθώς ο τομέας είναι ιδιαίτερα ευρύς και μια εργασία δεν είναι σε θέση να καλύψει όλα τα θέματα. Επίσης, στόχος της είναι ο ερεθισμός του αναγνώστη για αναζήτηση περισσότερων πληροφοριών πάνω στο αντικείμενο του Ηλεκτρονικού Φακέλου. Απευθύνεται σε λειτουργούς υγείας και διοικητικά στελέχη, τα οποία ενημερώνει σχετικά με χρήσιμα στοιχεία, όπως είναι τα Πληροφοριακά Συστήματα Υγείας, η χρήση των Ηλεκτρονικών Φακέλων Υγείας και η ασφάλεια των Προσωπικών Δεδομένων σε αυτές τις περιπτώσεις.

Βιβλιογραφία

Ελληνική Βιβλιογραφία

1. Αγγελόπουλος, Γ. (2012). Υλοποίηση Web Εφαρμογής για το Εθνικό Σύστημα Υγείας Προσανατολισμένη στην Καταπολέμηση της Φοροδιαφυγής και την Προστασία του Κρατικού Χρήματος. Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής, Πολυτεχνική Σχολή, Πανεπιστήμιο Πατρών.
2. Αποστολάκης, Ι. (2002). *Πληροφοριακά Συστήματα Υγείας*. Αθήνα: Παπαζήση.
3. Αραποστάθη, Μ. και Τζεμπετζή, Γ. (2004) “Ιατρικός Φάκελος Ασθενούς. Χειρόγραφο και ηλεκτρονικό σύστημα, διαπιστώσεις και επισημάνσεις”, *Περιοδικό Επιθεώρηση Υγείας* 15(87): 31-36
4. Ανσουριάν, Μ. (2011). Ολοκληρωμένα Πληροφοριακά Συστήματα για Ιδεώτες Ελεύθερους Επαγγελματίες στο Χώρο της Υγείας. Πανεπιστήμιο Μακεδονίας Οικονομικών και Κοινωνικών Επιστημών, Δ.Π.Μ.Σ. Εφαρμοσμένης Πληροφορικής, Τμήμα Επιχειρηματικής Πληροφορικής.
5. Γιούπιου, Ε. (2011). Ανάλυση και Σχεδιασμός Διαχείρισης Συστήματος Νοσοκομείου. Πανεπιστήμιο Πειραιώς, Τμήμα Πληροφορικής, ΜΠΣ "Προηγμένα Συστήματα Πληροφορικής".
6. Δεσκέρε, Ε. (2008). Πληροφοριακά Συστήματα Υγείας: Οι Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών στο Χώρο της Υγείας - Πρόνοιας. Μελέτη Περίπτωσης: Ένα Δημόσιο Νοσοκομείο Ίδρυμα. Τεχνολογικό Εκπαιδευτικό Ίδρυμα Μεσολογγίου, Σχολή Διοίκησης και Οικονομίας, Τμήμα Εφαρμογών Πληροφορικής στη Διοίκηση και Οικονομία.
7. Καλιμάνη, Δ. (2013). Δημιουργία Ιατρικού Φακέλου με Χρήση CMS. Ανάλυση Απαιτήσεων του Ιατρικού Φακέλου και των Συστημάτων του από τη Σκοπιά της Πληροφορικής και της Οικονομίας. Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών, Πληροφορικής Επιστημών Ζωής.
8. Κατόπουλος, Δ. & Τσιμπουκέλης, Κ. (2010). Αρχές και Εφαρμογές Διαλειτουργικότητας στην Ηλεκτρονική Υγεία. Εθνική Σχολή Δημόσιας Διοίκησης, Τμήμα Διαχείρισης Πληροφοριακών Συστημάτων.

9. Καρύδη, Β. (2010). Νέες τεχνολογίες στις κατ' οίκον υπηρεσίες υγείας. Πανεπιστήμιο Πατρών, Τμήμα Ιατρικής
10. Κιουντούζης, Ε. (2009). *Μεθοδολογίες Ανάλυσης & Σχεδιασμού Πληροφοριακών Συστημάτων*. Αθήνα: Μπένου.
11. Κούτρας, Σ. (2005). *Πειστικός Λόγος*. Αθήνα: Σαββάλας.
12. Λούσα, Δ. (2010). Κατανομημένο Ιατρικό Πληροφοριακό Σύστημα. Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης, Σχολή Τεχνολογικών Εφαρμογών, Τμήμα Εφαρμοσμένης Πληροφορικής και Πολυμέσων.
13. Μαγκλογιάννης, Η. (2013). Ηλεκτρονικός Φάκελος Υγείας για Υπολογιστές Παλάμης. Πανεπιστήμιο Αιγαίου, Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων.
14. Μαντάς Ι. Πανεπιστημιακές παραδόσεις στο μεταπτυχιακό πρόγραμμα Πληροφορική της Υγείας, Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών, 2004
15. Μπουραντάς, Δ. (2002). *Μάνατζμεντ. Θεωρητικό Υπόβαθρο, Σύγχρονες Πρακτικές*. Αθήνα: Μπένου.
16. Παπαδάκη, Β. (2007). *Στρατηγική των Επιχειρήσεων: Ελληνική και Διεθνής Εμπειρία*. Αθήνα: Μπένου.
17. Σαραντινού, Μ. (2013). Μελέτη Σύγχρονων Συστημάτων Παροχής Υψηλής Ποιότητας Τηλεϊατρικών Υπηρεσιών για χειρισμό και αντιμετώπιση των ιατρικών και υγειονομικών προβλημάτων στην Ελληνική Ναυσιπλοΐα. Εθνικό Μετσόβιο Πολυτεχνείο, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Τομέας Συστημάτων Μετάδοσης Πληροφορίας και Τεχνολογίας Υλικών.
18. Τσάκωνα, Α. (2009). Εκπαίδευση Επαγγελματιών Υγείας και Ορθή Εισαγωγή του Φακέλου Υγείας σε Δημόσια Νοσηλευτικά Ιδρύματα στην Ελλάδα και την Ευρωπαϊκή Ένωση. Πανεπιστήμιο Πατρών, Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών Πληροφορικής Επιστημών Ζωής.
19. Τσαλουκίδης, Ν. & Παπαγεωργίου, Δ. (2008). Ο ρόλος των Πληροφοριακών Συστημάτων Υγείας στην οργάνωση και διεκπεραίωση της νοσηλευτικής πρακτικής. *Νοσηλευτική, 2008, 47*.
20. Φαρατζιάν, Α. (2007). Στρατηγική & Ποιότητα Μονάδων & Υπηρεσιών Υγείας. Πανεπιστήμιο Πειραιώς, Τμήμα Οργάνωσης & Διοίκησης Επιχειρήσεων, Ευρωπαϊκό ΜΠΣ στη Διοίκηση Επιχειρήσεων - Ολική Ποιότητα.

21. Χατζηπαναγιώτη, Γ. (2009). Δημιουργία Συστήματος Ηλεκτρονικών Ιατρικών Φακέλων με Χρήση Έξυπνων Καρτών. Πανεπιστήμιο Αιγαίου, Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων.
22. Χουλιάρας, Δ. (2006). Πρότυπα Μοντέλα Αναφοράς, Αναπαράσταση Ηνωστικής Πληροφορίας Σχεδιαστικοί Περιορισμοί και Προδιαγραφές. Πανεπιστήμιο Πατρών, Τμήμα Ιατρικής, Εθνικό Μετσόβιο Πολυτεχνείο, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Η/Υ, Τμήμα Μηχανολόγων Μηχανικών.

Ξένη Βιβλιογραφία

1. Avison, D. & Fitzgerald, G. (2006). *Ανάπτυξη Προηγμένων Πληροφοριακών Συστημάτων: Μεθοδολογίες & Εργαλεία*. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.
2. Behrouz, F.A. & Firouz, M. (2010). *Εισαγωγή στην Επιστήμη των Υπολογιστών*. Αθήνα: Κλειδάριθμος.
3. Caudill-Slosberg, M., & Weeks, W. B. (2005). Case study: identifying potential problems at the human/technical interface in complex clinical systems. *American Journal of Medical Quality*, 20(6).
4. Deshpande, A., & Jadad, A. R. (2006). Web 2.0: Could it help move the health system into the 21st century?. *The journal of men's health & gender*, 3(4).
5. Dritsas, S., Gymnopoulos, L., Karyda, M., Balopoulos, T., Kokolakis, S., Lambrinoudakis, C., & Katsikas, S. (2006). A knowledge-based approach to security requirements for e-health applications. *Electronic Journal for E-Commerce Tools and Applications*.
6. European Committee (EC) for Standardization (2003). Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy. European Committee for Standardization.
7. Gunter, T. D., & Terry, N. P. (2005). The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions. *Journal of Medical Internet Research*, 7(1).
8. Häyrynen, K., K. Saranto, and P. Nykänen, Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics*, 2008. 77(5): p. 291-304.

9. Laudon, K.C. & Laudon, J.P. (2009). *Πληροφοριακά Συστήματα Διοίκησης. Διοίκηση της Ψηφιακής Επιχείρησης*. Αθήνα: Κλειδάριθμος.
10. Lluch, M., Healthcare professionals' organisational barriers to health information technologies—A literature review. *International Journal of Medical Informatics*, 2011. 80(12): p. 849-862.
11. Ludwick, D.A. and J. Doucette, Adopting electronic medical records in primary care: Lessons learned from health information systems implementation experience in seven countries. *International Journal of Medical Informatics*, 2009. 78(1): p. 22-31.
12. Shah, N. R., Seger, A. C., Seger, D. L., Fiskio, J. M., Kuperman, G. J., Blumenfeld, B., ... & Gandhi, T. K. (2006). Improving acceptance of computerized prescribing alerts in ambulatory care. *Journal of the American Medical Informatics Association*, 13(1).
13. Turban, E. & Volonino, L. (2012). *Information Technology for Management*. UK: John Wiley & Sons, Inc.
14. Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D. W., & Middleton, B. (2005). The value of health care information exchange and interoperability. *Health Affairs-Millwood va then Bethesda*, 24, W5.

Διαδικτυακές Πηγές

1. <http://www.nap.edu>
2. <http://healthnotesandnews.blogspot.gr/2010/04/1-1.html>
3. Health Level 7(www.hl7.org)
4. http://lentzas.blogspot.gr/2010/05/blog-post_3896.html
5. <http://sparta94.wordpress.com/page/2/>
6. http://www.meducator3.net/melinaplus/sites/default/files/EHR_Lesson2.pdf
7. http://plhroforikh-vioiatrikhtehnologia.blogspot.gr/p/blog-page_4643.html
8. <http://panacea.med.uoa.gr/topic.aspx?id=508>

