ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΚΑΤΕΥΘΥΝΣΗ: ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

«Ασφάλεια και Ιδιωτικότητα σε Πληροφοριακά Συστήματα Υγείας»

Διπλωματική Εργασία

Φοιτήτρια **Ευαγγελία Καρασταμάτη**

Επιβλέπων Καθηγητής **Κωνσταντίνος Λαμπρινουδάκης**

Αθήνα, Νοέμβριος 2012

ПАЦІЄНТ ПЕРАМ

Περίληψη

Η τεχνολογία πληροφοριών (ΤΠ) ήρθε προκειμένου να μετασχηματίσει τους τρόπους που τα σύγχρονα συστήματα της υγειονομικής περίθαλψης αποκτούν, αποθηκεύουν, έχουν πρόσβαση και διαβιβάζουν τις ιατρικές πληροφορίες. Αυτές οι εξελίξεις προσφέρουν σημαντικά οφέλη τόσο στους ασθενείς όσο και στο ιατρικό και νοσηλευτικό προσωπικό.

Το γεγονός αυτό οδηγεί μονοσήμαντα στην υιοθέτηση και εφαρμογή πληροφοριακών συστημάτων και τεχνολογιών πληροφορικής, προκειμένου να καταγραφεί και να γίνει επεξεργασία του μεγάλου όγκου των πληροφοριών και των δεδομένων, που προέρχονται τόσο από τις ιατρικές όσο και από τις διοικητικό-οικονομικές λειτουργίες των οργανισμών.

Η εργασία αυτή περιλαμβάνει θέματα που αφορούν τα πληροφοριακά συστήματα υγείας καθώς και εφαρμογές πληροφορικής στο τομέα αυτό. Στόχος της εργασίας είναι να κατανοήσουμε την έννοια των πληροφοριακών συστημάτων στον τομέα της υγείας. Στη συνέχεια, λοιπόν, παρουσιάζονται αναλυτικά οι λειτουργίες ενός Ολοκληρωμένου Πληροφοριακού Συστήματος Υγείας καθώς και τα διάφορα υποσυστήματα του.

Εν συνεχεία, γίνεται μια παρουσίαση των θεμάτων διαλειτουργικότητας και ανταλλαγής δεδομένων μεταξύ των Πληροφοριακών Συστημάτων στο χώρο της υγείας, ένα αντικείμενο που αποτελεί σημαντικό παράγοντα επιτυχίας και αξιοποίησης των Πληροφοριακών Υποδομών αυτών από τους επαγγελματίες υγείας. Μελετώνται λοιπόν συνοπτικά, τα διάφορα επίπεδα διαλειτουργικότητας και διερευνώνται τα πρότυπα και οι κωδικοποιήσεις που υφίστανται στον τομέα της υγείας.

Μέσα από την μεταπτυχιακή διπλωματική εργασία μελετείται και συζητείται η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των ασθενών, η προστασία των προσωπικών δεδομένων και η εξασφάλιση ενός υψηλού επιπέδου προστασίας κατά τη διασυνοριακή διακίνησή τους. Επιπλέον, παρουσιάζονται νομοθετικά ζητήματα που προκύπτουν από την εισαγωγή της τεχνολογίας στον χώρο της υγείας.

Το πρόβλημα της ασφάλειας των πληροφοριών και της προστασίας των προσωπικών δεδομένων είναι ιδιαίτερα σημαντικό στα σύγχρονα Πληροφοριακά Συστήματα και πρωτίστης προτεραιότητας στον τομέα της υγείας. Τα αρχεία υγείας ενός ασθενούς αποτελούν ιδιαίτερα ευαίσθητα προσωπικά δεδομένα. Λόγω της ευαισθησίας των προσωπικών στοιχείων είναι επιτακτική η ανάγκη να πληρούνται όλες εκείνες οι προϋποθέσεις ασφάλειας που θα εξασφαλίζουν το αδιάβλητο των δεδομένων. Η ασφάλεια των ευαίσθητων δεδομένων είναι ένα σημαντικότατο θέμα για το οποίο, ωστόσο, η τεχνολογία έχει δώσει ουσιαστικές λύσεις, οι οποίες μάλιστα μπορεί να θεωρηθούν αποτελεσματικότερες από αυτές που μέχρι σήμερα εφαρμόζονται για την τήρηση και φύλαξη των αρχείων υγείας των ασθενών. Στη συνέχεια λοιπόν της εργασίας

γίνεται μια ανασκόπηση των υφιστάμενων τάσεων όσον αφορά τις πτυχές τις ασφάλειας των ΠΣΥ.

Εν κατακλείδι, εξαιτίας της ευαισθησίας των ιατρικών δεδομένων, η ανάγκη για την επιλογή κατάλληλων μέτρων ασφάλειας συνεχώς και αυξάνεται και η διαδικασία επιλογής των μέτρων αυτών είναι μια επίπονη διαδικασία. Καταλήγοντας, γίνεται μια παρουσίαση της Ανάλυσης Κινδύνων, μια διαδικασία που αναγνωρίζει τα προβλήματα ασφαλείας, τα ταξινομεί με βάση την σημαντικότητα τους και τέλος προτείνει λύσεις για την επίλυση τους. Επιπλέον, παρουσιάζονται οι διαφορετικοί τρόποι ανάλυσης κινδύνων, οι κυριότερες μέθοδοι που χρησιμοποιούνται σήμερα, τα πακέτα λογισμικού που κυκλοφορούν στην αγορά και τελικά γίνεται μια πρακτική εφαρμογή ανάλυσης κινδύνων σε ένα υποτιθέμενο Ολοκληρωμένο Πληροφοριακό Σύστημα Υγείας ενός Περιφερειακού Δικτύου Υγείας με την μέθοδο CRAMM.

Λέξεις Κλειδιά

Ολοκληρωμένα Πληροφοριακά Συστήματα Υγείας, Διαλειτουργικότητα, Ασφάλεια Πληροφοριακών Συστημάτων Υγείας, Ανάλυση Κινδύνων.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Abstract

Information Technology (IT) came in order to convert the ways that modern systems of health care acquire, store, have access and transmit medical information. These developments offer significant benefits to both the patients and to the medical or nursing personnel.

This unambiguously, leads to the adoption and implementation of solutions such as information systems and information technologies, in order to record and process effectively this large amount of data that derive both from the medical and the administrative-economic operations of the organizations.

This dissertation includes issues related to health information systems and computer applications in this field. The aim of this study is to comprehend the meaning of information systems in the health sector. Therefore, the functions of an Integrated Health Information System and its various subsystems are presented.

Subsequently, we present the issues of interoperability and data exchange between health information systems, which are of critical matter for the success and utilization of IT Infrastructure from health professionals. Thus, the various levels of interoperability are studied briefly, as well as the standards and encodings that exist in the health sector.

In addition, through this study, matters such as the protection of patients' rights and fundamental freedoms, the protection of personal data and ensuring a high level of protection against cross-border transfer, are discussed. Moreover, we present legal issues arising from the introduction of technology in the healthcare sector.

The issues of information security and the protection of personal data are of high importance in modern Information Systems and of utmost priority in healthcare. Patients' medical records constitute particular sensitive data. Given the sensitivity of personal information, it is imperative to meet the requirements for data security and integrity. The security of sensitive data is an important issue for which technology has provided effective solutions, which may even be considered to be more effective than the ones that are currently applied for the maintenance and storage of patients' medical records. Thereafter, we present an overview of the current trends in relation to the security aspects of Health Information Systems.

Finally, because of the sensitivity of medical data, the need for selecting appropriate security countermeasures is constantly increasing and the procedures for selecting these measures is considered a tedious process. In the end, we present the Risk Analysis method, a process that identifies and classifies the security issues based on their significance and finally proposes solutions to resolve them. Furthermore, we present the different ways of the Risk Analysis process, the main methods that are currently used and the software packages that are available on the market. To conclude, we present a practical implementation of the Risk Analysis process

using CRAMM, on a supposing Integrated Health Information System of a Regional Health Network.

Key Words

Integrated Health Information Systems, Interoperability, Health Information Systems Security, Risk Analysis

INFOTHEO&TECH

ПРЕЗЕНТАЦИЯ

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών με τίτλο «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων».

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η κατανόηση της λειτουργίας των Πληροφοριακών Συστημάτων Υγείας και των διάφορων υποσυστημάτων τους. Επιπλέον, επιχειρείται η εφαρμογή της διαδικασίας Ανάλυσης Κινδύνων με την μέθοδο CRAMM στην υλοποίηση ενός υποτιθέμενου Ολοκληρωμένου Πληροφοριακού Συστήματος Υγείας, τμήματος ενός Περιφερειακού Δικτύου Υγείας.

Στο σημείο αυτό, θα ήθελα να εκφράσω τις ευχαριστίες μου σε όσους συνετέλεσαν στην ολοκλήρωση αυτής της εργασίας. Θα ήθελα να ευχαριστήσω, ιδιαίτερα, τον επιβλέποντα καθηγητή κύριο Κωνσταντίνο Λαμπρινουδάκη, για την καθοδήγηση που μου προσέφερε και τις πολύτιμες συμβουλές του κατά την εκπόνηση της εργασίας μου. Επίσης, θα ήθελα να ευχαριστήσω τα μέλη τις εξεταστικής επιτροπής που μου έκαναν της τιμή να αξιολογήσουν την προσπάθειά μου. Συνεχίζοντας, όλους εκείνους που με την συνεισφορά τους έκαναν δυνατή την επιτυχημένη ολοκλήρωση αυτής της εργασίας. Τέλος, θα ήθελα να ευχαριστήσω τη μητέρα μου, της οποίας η ανεκτίμητη βοήθεια και αγάπη όλα αυτά τα χρόνια, θεωρώ πως είναι οι παράγοντες που με στήριξαν στην επίτευξη των στόχων μου.

Νοέμβριος 2012

Ευαγγελία Καρασταμάτη

ПРЕДВАРИТЕЛЬНО

Περιεχόμενα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

ПРЕДВАРИТЕЛЬНО

Κεφάλαιο 1

Πληροφοριακά Συστήματα Υγείας – Αποσαφήνιση όρων

1.1 Εισαγωγή

Ιστορικά, ο τομέας της υγείας αποτελούνταν από ανεξάρτητες, αυτόνομες μονάδες με μικρή ως ελάχιστη ανταλλαγή δεδομένων και πληροφοριών μεταξύ τους, ενώ η χρήση Τεχνολογιών και Πληροφορικής αντιμετωπίσθηκε επίσης αυτόνομα και κατά περίπτωση. Στην σημερινή εποχή όμως, η πίεση για αλλαγές και βελτιώσεις αυξάνεται ολοένα και περισσότερο. Παράλληλα, από πλευράς πολιτείας απαιτείται πλέον αποδοτικότητα και ελαχιστοποίηση του κόστους με ταυτόχρονη αύξηση της ποιότητας των παρεχόμενων υπηρεσιών.

Με δεδομένη λοιπόν την πολυπλοκότητα του χώρου, την πανσπερμία διαφορετικών τεχνολογικών λύσεων, την εξειδίκευση των πληροφοριακών συστημάτων και την πολυπλοκότητα της διακινούμενης πληροφορίας, είναι ιδιαίτερα δύσκολο στο να δοθούν σαφείς ορισμοί σχετικά με τα πληροφοριακά συστήματα που σχεδιάζονται για τον χώρο αυτόν. Στην διεθνή βιβλιογραφία, επικρατεί μία σύγχυση καθώς η ακριβής σημασία των όρων που χρησιμοποιούνται διαφοροποιείται ανάλογα με τον συγγραφέα, ερευνητή ή μελετητή. Στο κεφάλαιο αυτό θα αναφερθούμε στην ιστορική εξέλιξη των Πληροφοριακών Συστημάτων Υγείας (ΠΣΥ) και θα επισημάνουμε μερικούς από τους επικρατέστερους ορισμούς. Παράλληλα, θα προσπαθήσουμε να τους δομήσουμε με τρόπο τέτοιον ώστε να γίνει κατανοητό το πλαίσιο μέσα στο οποίο λειτουργούν και αναπτύσσονται οι τεχνολογίες της πληροφορικής.

1.2 Ορισμοί και Στόχοι Ολοκληρωμένων Πληροφοριακών Συστημάτων Υγείας

Μερικοί από τους ορισμούς που έχουν δοθεί κατά καιρούς από διάφορους συγγραφείς για τον προσδιορισμό της έννοιας του πληροφοριακού συστήματος στον τομέα της υγείας αναφέρουν, σύμφωνα με Lederer και Salmela, (Mohd et al. 2008) ότι η εισαγωγή, η επεξεργασία και η παραγωγή είναι στοιχεία που διαμορφώνουν ένα σύστημα. Ένα σύστημα περιλαμβάνει επίσης έναν συνδυασμό μεταβλητών ή συστατικών που είναι αλληλένδετες, οργανωμένες και εξαρτάται το ένα από το άλλο. Ο Beaumont (2008) αναφέρει ότι όλα τα πληροφοριακά συστήματα περιλαμβάνουν: Input(s), Process(es), Output(s), και Boundary.

Σύμφωνα με τον Κίτσιου (2010) τα ολοκληρωμένα πληροφοριακά συστήματα υγείας περιλαμβάνουν ένα ευρύτερο φάσμα πληροφοριακών συστημάτων και υποσυστημάτων, για αποθήκευση, οργάνωση, εξαγωγή και διαχείριση ιατρικών και διοικητικών πληροφοριών προκειμένου να εκτελεστούν αυτές οι εργασίες αποδοτικά και αποτελεσματικά.

Με την έννοια Ιατρικό Πληροφοριακό Σύστημα ορίζουμε ένα ολοκληρωμένο σύστημα πληροφοριών ιατρικού ενδιαφέροντος. Έτσι πρέπει να υπάρχουν ψηφιακές πληροφορίες τόσο διοικητικού-οικονομικού όσο και ιατρικού, εργαστηριακού ενδιαφέροντος, δομημένες με τέτοιον τρόπο ώστε να επιτρέπεται η γρήγορη, ακριβής και ασφαλής ενημέρωση ή συλλογή πληροφορίας (Παρατηρητήριο για την κοινωνία της πληροφορίας, 2007; Βαγγελάτος, Α. 2001; Καρπουζής, Κ. 2004).

Σύμφωνα με τον Αποστολάκη (2002), ένα ολοκληρωμένο πληροφοριακό σύστημα είναι το περιβάλλον στο οποίο τηρούνται όλες οι πληροφορίες που σχετίζονται με τον ασθενή (εξετάσεις που απαιτούνται, αποτελέσματα εξετάσεων κλπ) και οι οποίες διοχετεύονται αυτόματα (σαν δεδομένα) σε άλλες λειτουργίες-επεξεργασίες (π.χ. πληρωμή νοσηλειών).

Ένα σύστημα πληροφοριών υγείας είναι ένα ακέραιο συστατικό οποιουδήποτε συστήματος υγειονομικής περίθαλψης. Παρέχει το πλαίσιο μέσα στο οποίο η συλλογή δεδομένων, η επεξεργασία, η ανάλυση και η υποβολή έκθεσης των πληροφοριών υγείας πραγματοποιούνται και διευκολύνουν την ανάπτυξη των κατάλληλων δεικτών υγειονομικής περίθαλψης για τον έλεγχο και την αξιολόγηση της απόδοσης του συστήματος υγειονομικής περίθαλψης (Matshidze, P., Hanmer, L., http://www.hst.org.za/uploads/files/chap6_07.pdf).

Καταλήγοντας, επιγραμματικά θα αναφέρουμε μερικούς από τους στόχους των ΠΣΥ:

- Ψηφιακή διαχείριση και επεξεργασία ιατρικής πληροφορίας.
- Διασύνδεση τμημάτων και φορέων παροχής υπηρεσιών υγείας.
- Να υποστηρίζουν τον γιατρό, τη νοσοκόμα και το διοικητικό προσωπικό αλλά κυρίως να ενισχύουν τον ασθενή και τον πολίτη σε θέματα υγείας.
- Διαχείριση της ιατρική πληροφορίας για την προαγωγή της υγείας και τη διαχείριση του ασθενούς, αλλά και για την υποστήριξη κλινικής έρευνας, βασικής έρευνας και εκπαίδευσης.
- Να δώσουν τεχνικές λύσεις για ψηφιακή διαχείριση πληροφορίας, αλλά κυρίως να υποστηρίζουν ροή εργασίας και μακροπρόθεσμη διαχείριση και στρατηγική ανάπτυξη οργανισμών υγείας.
- Να διαχειριστούν νέα είδη πληροφορίας (π.χ. γονιδιακή) και να χρησιμοποιήσουν νέα είδη τεχνολογίας (π.χ. συσκευές που φέρονται στο σώμα).

1.3 Ιστορία και εξέλιξη

Η τεχνολογία της πληροφορικής χρησιμοποιήθηκε για πρώτη φορά σε νοσοκομεία, την δεκαετία του 1940, για να καλύψει αρχικά ανάγκες διοικητικής και οικονομικής φύσης. Συστήματα που αναφέρονταν στην διαχείριση πληροφοριών σχετικά με τους ασθενείς εμφανίστηκαν στα μέσα του 1960 (Hammond 1994). Ο πρώτος στόχος αυτών των συστημάτων ήταν η απλοποίηση της επικοινωνίας και της τεκμηρίωσης μέσα από την χρήση τυποποιημένων παραγγελιών και σχεδίων περίθαλψης και θεραπείας (Ozbolt 2001).

Κατά την περίοδο 1970–1980, στην οποία έγινε και η εμφάνιση των μικροϋπολογιστών, τα πληροφοριακά συστήματα άρχισαν να περιλαμβάνουν εφαρμογές για την υποστήριξη των οικονομικών και διοικητικών διαδικασιών ενός νοσοκομείου. Επίσης, κατά την περίοδο αυτή, εκτός από την εμφάνιση των μικροϋπολογιστών, άρχισε και η χρήση των βάσεων δεδομένων η οποία έδωσε την δυνατότητα άμεσης διαθεσιμότητας των δεδομένων και παραγωγής αναφορών. Τα συστήματα αυτά ήταν κατά κύριο λόγο εφαρμογές, η λειτουργία και η χρησιμότητα των οποίων περιορίζονταν στα πλαίσια ενός συγκεκριμένου λειτουργικού τμήματος (stand-alone). Συνήθως, βασίζονταν σε τοπικές βάσεις δεδομένων ενώ η δυνατότητα σύνδεσης μεταξύ τους αντιμετωπιζόταν ως δευτερεύον θέμα.

Ο κρίσιμος σταθμός, χρονικά, είναι τα μέσα της δεκαετίας του 80’ αφού τότε γίνεται ευρέως εφικτή η αξιόπιστη και απαλλαγμένη από σφάλματα μετάδοση δεδομένων σε υψηλές ταχύτητες ανεξαρτήτως είδους και ιδιαίτερων χαρακτηριστικών αυτών. Ταυτόχρονα με την χρήση των τοπικών δικτύων υπολογιστών (Local Area Networks-LAN), η διάδοση των προσωπικών υπολογιστών ενίσχυσε την εγκατάστασή τους σε μεγάλο αριθμό νοσοκομείων. Έτσι, πολλοί προμηθευτές πληροφοριακών συστημάτων αναγκάστηκαν να δώσουν στα συστήματά τους τη δυνατότητα επικοινωνίας με άλλα συστήματα. Επίσης, κατά το χρονικό αυτό διάστημα άρχισε και η θεμελίωση των πρώτων προτύπων λειτουργικών συστημάτων, πρωτοκόλλων δικτύων και συστημάτων διαχείρισης αρχείων δεδομένων. Ως αποτέλεσμα, οι προμηθευτές ΠΣΥ άρχισαν να χρησιμοποιούν συστήματα διαχείρισης βάσεων δεδομένων άλλων προμηθευτών, μερικά από τα οποία συμπεριλάμβαναν και γλώσσες διαχείρισης δεδομένων μέσω των οποίων δινόταν η δυνατότητα ανάκτησης δεδομένων που διαχειρίζονταν άλλες εφαρμογές.

Από το 1991 έως σήμερα, έχει αρχίσει να εμφανίζεται μια νέα γενιά πληροφοριακών συστημάτων, αν και τα χαρακτηριστικά της προηγούμενης γενιάς δεν έχουν εκλείψει εντελώς. Υπάρχουν διάφοροι παράγοντες που επηρεάζουν τη γενιά αυτή, όπως η αύξηση της δυνατότητας σύνδεσης δικτύων υπολογιστών, η δυνατότητα εγκατάστασης και χρήσης ενός συστήματος διαχείρισης βάσεων δεδομένων σε περισσότερα από ένα σημεία και η αύξηση και η καθιέρωση προτύπων στη λειτουργία των πληροφοριακών συστημάτων. Με τον όρο πρότυπο, εννοούμε τον κοινό τρόπο θεώρησης και αντιμετώπισης ενός συγκεκριμένου θέματος. Έτσι,

στον χώρο της πληροφορικής στο διάστημα αυτό εμφανίστηκαν πρότυπα επικοινωνίας υπολογιστών, παραγωγής δεδομένων κλπ, τα οποία έδωσαν τη δυνατότητα επικοινωνίας διαφορετικών πληροφοριακών συστημάτων (στο ίδιο γεωγραφικό σημείο ή σε διαφορετικά).

Η εξέλιξη των υπολογιστικών συστημάτων στον χώρο της υγείας υπήρξε αρκετά αργή σε σχέση με την διείσδυση των συστημάτων αυτών στις επιχειρήσεις και στην βιομηχανία (Kazanjian 1998). Υπάρχουν πολλές αιτίες για αυτήν την καθυστέρηση (Grimson 2000), ανάμεσα στις οποίες συμπεριλαμβάνονται, η έλλειψη επενδύσεων, η έλλειψη πολιτικής θέλησης, η αδυναμία της αγοράς να καλύψει τις απαιτήσεις των ιδρυμάτων, καθώς και η έλλειψη ή η πολύ αργή υιοθέτηση προτύπων. Επιπλέον υπάρχουν προβλήματα που σχετίζονται ειδικά με τον χώρο της υγείας, όπως η πολυπλοκότητα των ιατρικών δεδομένων, προβλήματα με την είσοδο των δεδομένων, θέματα ασφάλειας και εμπιστευτικότητας, η έλλειψη σε πολλές χώρες ενός κωδικού που να αντιστοιχεί με τρόπο μοναδικό σε κάθε έναν ασθενή (unique patient identifier), και η γενικότερη έλλειψη ενημέρωσης σχετικά με τα πλεονεκτήματα αλλά και τους κινδύνους των πληροφοριακών συστημάτων στην υγεία.

Στις μέρες μας, όμως, γίνεται ολοένα και περισσότερο κοινή η πεποίθηση ότι το επίπεδο ανάπτυξης των συστημάτων πληροφορικής που χρησιμοποιούνται σε ένα νοσοκομειακό ίδρυμα, δεν αποτελεί απλώς μια τεχνολογική πολυτέλεια ή μια απλή διευκόλυνση, αλλά ότι συνδέεται άμεσα με το επίπεδο της παρεχόμενης περίθαλψης. Σαν αποτέλεσμα αυτής της συνειδητοποίησης, η ανάπτυξη και η εφαρμογή τέτοιων συστημάτων προωθείται πλέον από όλους τους παράγοντες που σχετίζονται με την λειτουργία των νοσοκομείων, και υπάρχει έντονη ερευνητική δραστηριότητα που σχετίζεται με το θέμα αυτό.

1.4 Τύποι Πληροφοριακών Συστημάτων Υγείας

Ο στόχος ενός Πληροφοριακού Συστήματος Υγείας (ΠΣΥ) είναι να βελτιωθεί η δυνατότητα να συλλεχθούν, να αποθηκευτούν και να αναλυθούν ακριβή δεδομένα υγείας, η αποδοτικότητα παροχής υπηρεσιών, η βελτίωση ακρίβειας δεδομένων, η αποτελεσματικότητα της επέμβασης, η αύξηση της υπευθυνότητας και η ενημέρωση για νέες τάσεις. Η βελτιστοποίηση της ποιότητας των υπηρεσιών και παροχή επίκαιρων και ορθών πληροφοριών έχει ως αποτέλεσμα τον καλύτερο προγραμματισμό υγειονομικής περίθαλψης, την βελτιωμένη διάγνωση και την πρόσβαση περισσότερων ασθενών σε υπηρεσίες υγείας για μια ολόκληρη χώρα (Haux et al. (2004); Tan (2002)).

Ένα ΠΣΥ περιγράφει συνήθως ένα από αυτά τα διακριτά υποσυστήματα που περιέχουν τα εξής στοιχεία (WHO, 2005):

- Επιτήρηση ασθενειών και κοινοποίηση αυτών σε περίπτωση ξεσπάσματος.

- Δεδομένα που εξάγονται μέσω οικιακών ερευνών.
- Καταγραφή και απογραφή σημαντικών γεγονότων (γεννήσεις, θάνατοι και αιτίες θανάτου).
- Συλλογή δεδομένων βασισμένη στα αρχεία ασθενών και υπηρεσιών και την υποβολή έκθεσης από τους δημόσιους εργαζομένους στον ιατρικό κλάδο, τους εργαζομένους στον ιατρικό κλάδο και τις υγειονομικές εγκαταστάσεις.
- Ειδικευμένα προγράμματα για έλεγχο και αξιολόγηση (πχ για TB, HIV/AIDS και EPI).
- Διαχείριση διοίκησης και πόρων (συμπεριλαμβανομένου του προϋπολογισμού, του προσωπικού, και των προμηθειών).

1.4.1 Νοσηλευτικά Πληροφοριακά Συστήματα

Τα νοσηλευτικά πληροφοριακά συστήματα είναι πακέτα λογισμικού που έχουν αναπτυχθεί για να χρησιμοποιούνται ειδικά από νοσηλευτές. Τα προγράμματα αυτά είτε αφορούν ένα συγκεκριμένο χώρο της νοσηλευτικής είτε υποστηρίζουν γενικότερα τις υπηρεσίες νοσηλευτικής διοίκησης. Παραδείγματα νοσηλευτικών τομέων που μπορούν να ωφεληθούν από τη μοναδική υποστήριξη των πληροφοριακών συστημάτων είναι μεταξύ άλλων, η ψυχική υγεία, η νεογνολογία, η ουρολογία, η ογκολογία, η μαιευτική, η χειρουργική και ο έλεγχος λοιμώξεων.

Τα γενικά νοσηλευτικά πληροφοριακά συστήματα διαθέτουν πολλαπλά προγράμματα ή μοντέλα, που χρησιμοποιούνται για να επιτελούν διάφορες κλινικές, εκπαιδευτικές και διαχειριστικές λειτουργίες. Τα περισσότερα από αυτά διαθέτουν μοντέλα για την ταξινόμηση των ασθενών, τη στελέχωση, τον προγραμματισμό των υπηρεσιών, τη διοίκηση προσωπικού και τη σύνταξη εκθέσεων. Μπορούν να ενταχθούν και άλλα μοντέλα όπως η κατάρτιση προϋπολογισμών, η κατανομή πόρων, ο έλεγχος του κόστους, η διαχείριση της ποιότητας, η ανάπτυξη προσωπικού, η διαμόρφωση μοντέλων και η προσομοίωση για την λήψη αποφάσεων, ο στρατηγικός σχεδιασμός, οι βραχυπρόθεσμες ανάγκες για την πρόβλεψη και σχεδιασμό εργασίας και η αξιολόγηση προγράμματος.

Τα μοντέλα για την ταξινόμηση ασθενών, την στελέχωση, τον προγραμματισμό των υπηρεσιών, τη διοίκηση προσωπικού και τη σύνταξη εκθέσεων συχνά σχετίζονται στενά μεταξύ τους. Οι ασθενείς ταξινομούνται σύμφωνα με τα καθιερωμένα κριτήρια βαρύτητας της κατάστασης. Οι πληροφορίες για την ταξινόμηση των ασθενών αποτελούν είσοδο για το μοντέλο που αφορά την απαιτούμενη στελέχωση υπηρεσιών και τα επίπεδα στελέχωσης υπολογίζονται με βάση διάφορους τύπους υπολογισμού του φόρτου εργασίας. Επίσης, η πραγματική στελέχωση αποτελεί και αυτή είσοδο και μπορεί να γίνει σύγκριση της απογραφής, της βαρύτητας της κατάστασης των ασθενών, της απαιτούμενης στελέχωσης και της πραγματικής στελέχωσης. Ο προϋπολογισμός υποστηρίζεται από την απογραφή, τη βαρύτητα της κατάστασης του ασθενούς

και από τα απαιτούμενα μοντέλα στελέχωσης. Οι πληροφορίες αυτές είναι πολύτιμες στην υποστήριξη αιτημάτων για επιπλέον προσωπικό, πλήρους ή μερικής απασχόλησης. Το μοντέλο της σύνταξης εκθέσεων δίνει τη δυνατότητα ανάκλησης όλων των καταχωρημένων πληροφοριών με έγκαιρο και παρουσιάσιμο τρόπο.

Τα νοσηλευτικά πληροφοριακά συστήματα μπορούν να χρησιμοποιηθούν για να κάνουν τη φροντίδα του ασθενούς πιο αποτελεσματική και οικονομική. Τα κλινικά στοιχεία περιλαμβάνουν το ιστορικό και την εκτίμηση του ασθενούς, τα σχέδια νοσηλευτικής φροντίδας, σημειώσεις και διαγράμματα νοσηλευτικής προόδου, παρακολούθηση των ασθενών, και σχεδιασμό της εξόδου από το ίδρυμα. Αυτά όλα μπορούν να γίνουν στο σταθμό του νοσηλευτή ή σε πιο προοδευτικά συστήματα, κοντά στον ασθενή.

Οι κλινικοί νοσηλευτές μπορούν να χρησιμοποιήσουν το νοσηλευτικό πληροφοριακό σύστημα για να αντικαταστήσουν χειρόγραφα συστήματα καταγραφής δεδομένων. Αυτό μπορεί να οδηγήσει σε μείωση του κόστους, ενώ παράλληλα μπορεί να δοθεί δυνατότητα για βελτιωμένη ποιότητα φροντίδας καθώς και ποιότητας ζωής. Οι κλινικοί νοσηλευτές μπορούν να συγκεντρώνουν και να καταχωρούν κλινικά δεδομένα, να χρησιμοποιούν τους Η/Υ για να τα αναλύουν και να τα καταρτίζουν και κατά συνέπεια να λαμβάνουν αποφάσεις ώστε να υποστηρίζουν τις κλινικές κρίσεις τους. Η αυτοματοποιημένη παροχή συμβουλών μπορεί να εφαρμοστεί στην οθόνη για να διαπιστωθούν αρνητικές αντιδράσεις σε φάρμακα, αλληλεπιδράσεις και προετοιμασία των σωστών δόσεων. Οι Η/Υ μπορούν με τον κατάλληλο προγραμματισμό να απορρίπτουν εντολές που μπορούν να δημιουργήσουν προβλήματα σε αυτούς και άλλους τομείς, αποτρέποντας, έτσι, τη δημιουργία λαθών.

1.4.2 Πληροφοριακά Συστήματα Διαγνωστικών Κέντρων

Τα διαγνωστικά κέντρα αποτελούν οργανισμούς ή επιχειρήσεις κερδοσκοπικού χαρακτήρα που δραστηριοποιούνται στον ιατρικό χώρο με επιτυχία προσφέροντας ιατρικές υπηρεσίες υψηλού ποιοτικού επιπέδου. Σκοπός τους είναι η έγκυρη και έγκαιρη διάγνωση για πρόληψη και θεραπεία προβλημάτων υγείας. Επιπλέον, στόχος τους αποτελεί η παροχή υπηρεσιών κάτω από άριστες συνθήκες, με ιδιαίτερη φροντίδα, συνέπεια και επιστημονική πληρότητα. Τα διαγνωστικά κέντρα έκαναν την εμφάνισή τους από το 1980 και μετά. Ραγδαία ήταν η ανάπτυξη τους στην Ελλάδα τα τελευταία χρόνια και πιο συγκεκριμένα στην περίοδο 1990-1995. Σήμερα ο συνολικός αριθμός των διαγνωστικών κέντρων που λειτουργούν στη χώρα μας εκτιμάται ότι αγγίζει τα 400.

Η χρήση των πληροφοριακών συστημάτων στα διαγνωστικά κέντρα είναι αναγκαία. Παρόλο που το πεδίο των υπηρεσιών τους είναι μικρότερο από αυτό των νοσοκομείων, κρίνεται απαραίτητη η ύπαρξη πληροφοριακών συστημάτων. Οι νοσηλευτικές υπηρεσίες διευκολύνονται μέσω του

σύγχρονου τεχνολογικού εξοπλισμού και των πληροφοριακών συστημάτων που εφαρμόζονται. Πολλές χειρονακτικές εργασίες αυτοματοποιούνται, με αποτέλεσμα η επεξεργασία των δεδομένων και οι διάφορες διεργασίες να γίνονται πολύ ταχύτερα. Η γρηγορότερη, λοιπόν, διεκπεραίωση των εργασιών συνεπάγεται την καλύτερη οικονομική και διοικητική οργάνωση του διαγνωστικού κέντρου. Τα έσοδα και οι δαπάνες προϋπολογίζονται και υπολογίζονται με τον καλύτερο δυνατό τρόπο, συνεπώς γίνεται αποτελεσματικότερη η διαχείριση των οικονομικών του κέντρου.

Επιπλέον, στην καλύτερη εφαρμογή των πληροφοριακών διαγνωστικών συστημάτων συντελεί η καταχώρηση των προσωπικών δεδομένων των ασθενών σε ιατρικούς φακέλους με την ταυτόχρονη επικοινωνία με τους άλλους τομείς του συστήματος. Υλοποιείται σε διάφορα κέντρα ηλεκτρονική εφαρμογή που δίνει την δυνατότητα στους γιατρούς να διαχειρίζονται και να επεξεργάζονται τον Ηλεκτρονικό Ιατρικό Φάκελο ασθενών. Ο γιατροί μέσω ηλεκτρονικού υπολογιστή θα μπορούν να δουν, περισσότερο στο μέλλον, και να επεξεργαστούν το ιστορικό και τα δημογραφικά στοιχεία του ασθενούς καθώς επίσης και τα αποτελέσματα των εργαστηριακών εξετάσεων. Ακόμη, η χρήση πληροφοριακών συστημάτων υποστηρίζει την εφαρμογή της τηλεϊατρικής και των έμπειρων συστημάτων και στα διάφορα διαγνωστικά κέντρα με τη διαφορά από τα νοσοκομειακά ιδρύματα ότι το πεδίο παροχής ιατρικών υπηρεσιών στα διαγνωστικά κέντρα είναι πιο περιορισμένο.

Σε πολλά διαγνωστικά κέντρα χρησιμοποιούνται κάποιες εφαρμογές που αποτελούν μερικώς πληροφοριακά συστήματα. Αναπτύσσονται υψηλής απόδοσης μαζικής αποθήκευσης συστήματα που συνδυάζουν την ταχύτητα των παράλληλων συστημάτων και την λειτουργικότητα της μαζικής αποθήκευσης με ιεραρχική δομή. Το αποτέλεσμα είναι συστήματα με ανοιχτή αρχιτεκτονική, προσβάσιμη από οποιοδήποτε δίκτυο που υποστηρίζει γνωστά πρότυπα. Δίνεται, έτσι, η δυνατότητα ανάπτυξης συστημάτων ικανών να αποθηκεύσουν μεγάλους όγκους πληροφορίας (ιατρικός φάκελος) με δυνατότητα άμεσης ανάκτησης και αποθήκευσης δεδομένων. Το προγράμματα αυτά εκτός των άλλων προσφέρουν :

- Ανοιχτή αρχιτεκτονική για εύκολη πρόσβαση.
- Κατασκευή συστημάτων από χαμηλού κόστους αποθηκευτικά μέσα.
- Είναι εφαρμόσιμα σε διάφορα συστήματα.
- Απεριόριστο αριθμό συνδέσεων.
- Κλιμακωτή απόδοση στη διαδικασία μετάπτωσης αρχείων.
- Συνεργάσιμα με τα πιο γνωστά είδη αποθηκευτικών μέσων.

Οι υπηρεσίες που προσφέρονται από τέτοιου είδους εφαρμογές είναι:

- Ασφαλής αποθήκευση και ανταλλαγή ιατρικών αρχείων σε πραγματικό χρόνο.
- Ασφαλής σύνδεση με τον φάκελο του ασθενούς μέσω κινητού τηλεφώνου τρίτης γενεάς.

- Φιλικές προς τον χρήστη διαδικασίες ώστε να γίνεται προσιτό ακόμα και στον άπειρο χρήστη.

Για την υλοποίηση τέτοιων εφαρμογών, συστημάτων υπάρχει συνεργασία μεταξύ οργανισμών από Γαλλία, Ιταλία και Ελλάδα.

Η ραγδαία εξέλιξη της τεχνολογίας ανεβάζει καθημερινά το επίπεδο των διαγνωστικών κέντρων. Σκοπός τους, λοιπόν, είναι να είναι πρωτοπόρα και σε αυτόν τον τομέα που ονομάζεται τεχνολογία και που είναι σημαντικότατος στον χώρο της υγείας. Προγράμματα και εφαρμογές που αποτελούν μερικώς πληροφοριακά συστήματα σίγουρα συνεισφέρουν με τον καλύτερο τρόπο προς αυτόν τον σκοπό εφόσον η χρήση ολοκληρωμένων πληροφοριακών συστημάτων δεν είναι ακόμη διαδεδομένη και εφικτή.

1.4.3 Πληροφοριακά Συστήματα Εργαστηρίων

Τα εργαστηριακά πληροφοριακά συστήματα (Laboratory Information Systems) είναι λογισμικό εγκατεστημένο σε ηλεκτρονικό υπολογιστή, ο οποίος είναι συνδεδεμένος με τον κατάλληλο ιατρικό εξοπλισμό. Είναι υπεύθυνα για την αποθήκευση κλινικών δεδομένων, την επαλήθευση της ακρίβειας των εξετάσεων, τη βαθμονόμηση των οργάνων, τη δημιουργία ή ενημέρωση αρχείων ασθενών, τη συλλογή πληροφοριών από ένα πλήθος συσκευών όπως συσκευές ανάλυσης αίματος. Οι ιατρικές συσκευές που πραγματοποιούν τις διάφορες μετρήσεις ονομάζονται εργαστηριακοί αναλυτές και διαθέτουν μικροεπεξεργαστές, που ελέγχουν και συντονίζουν τη σωστή λειτουργία των συσκευών. Ο χρήστης μπορεί να μεταφέρει την ίδια στιγμή ηλεκτρονικά στο εργαστηριακό πληροφοριακό σύστημα τις μετρήσεις από τις συσκευές. Οι χρησιμοποιούμενοι εργαστηριακοί αναλυτές διασυνδέονται στο όλο σύστημα μέσω ειδικών διατάξεων, που συνδέονται σε Η/Υ και το σύστημα, έτσι, αποτελεί ενιαίο κορμό παραγωγής.

Ένα ιδανικό ολοκληρωμένο πληροφοριακό σύστημα εργαστηρίων για να είναι καταξιωμένο στον ιατρικό χώρο χρειάζεται να είναι προσαρμοσμένο στις ανάγκες και τις ιδιαιτερότητες των εργαστηρίων κάθε νοσοκομείου ή διαγνωστικού κέντρου. Γενικά χαρακτηριστικά ενός πληροφοριακού εργαστηριακού συστήματος είναι:

- Μονόδρομη και αμφίδρομη επικοινωνία με πληθώρα αυτόματων αναλυτών.
- Παραγγελία εργαστηριακών εξετάσεων σε πραγματικό χρόνο.
- Έγκριση και ανάγνωση αποτελεσμάτων σε πραγματικό χρόνο.
- Δυνατότητα σύνδεσης αποτελεσμάτων και διαγνώσεων.
- Διαχείριση ποιότητας ιατρικών συσκευών.
- Παρακολούθηση αναλώσιμων.
- Στατιστική ανάλυση.

Σ' ένα τέτοιο σύστημα το λογισμικό είναι δομημένο με τη συλλογιστική πολλών χρηστών, που ο καθένας έχει διαφορετικές αρμοδιότητες και προσβάσεις στις διακινούμενες πληροφορίες. Διαθέτει πλήρη παραμετροποίηση επιτρέποντας το διαχωρισμό του συνόλου των εργαστηρίων σε επί μέρους τμήματα, τον καθορισμό του προσωπικού του τμήματος όπως και τις εξετάσεις που πραγματοποιεί το κάθε τμήμα. Διαχειρίζεται το ιστορικό των εξετάσεων όλων των ασθενών παρακολουθώντας τις εξετάσεις ανά ασθενή, τμήμα εργαστηρίου, κλινική, ασφαλιστικό φορέα και προαιρετικά μπορεί να εκτελεί τιμολογήσεις και να παρακολουθεί όλα τα σχετικά οικονομικά στοιχεία.

Ένα δίκτυο υπολογιστών απλώνεται στα τμήματα των εργαστηρίων. Οι καθημερινές εξετάσεις εισάγονται στο σύστημα είτε από κάθε κλινική, είτε από την γραμματεία των εργαστηρίων (τμήμα παραλαβής δειγμάτων). Σημαντικό είναι ότι ένα τέτοιο σύστημα μπορεί να υποβοηθά στην κατάργηση των πολλαπλών σημείων παραλαβής δειγμάτων καθώς και για παράδειγμα, στην κατάργηση πολλαπλών αιμοληψιών που παρατηρούνται στον ίδιο ασθενή κατά τη διάρκεια της ημέρας, για τις ανάγκες του κάθε εργαστηριακού τμήματος. Επιπλέον, από τα διάφορα τερματικά που τοποθετούνται, οι θεράποντες ιατροί παρακολουθούν το ιστορικό του ασθενούς, ενώ τα τρέχοντα αποτελέσματα διατίθενται στο τερματικό αμέσως μετά την ολοκλήρωση των εργαστηριακών διαδικασιών και ακολουθεί η έγκρισή τους από τους διευθυντές του κάθε εργαστηριακού τομέα, σε πραγματικό χρόνο και χωρίς καθυστερήσεις. Οι ασθενείς πλέον δεν συγκεντρώνονται στα εργαστήρια αναμένοντας τα αποτελέσματά τους ενώ η εικόνα της πορείας του ασθενούς είναι εμφανής και ευδιάκριτη. Οφέλη που προκύπτουν από τη χρήση του συστήματος είναι:

- Μείωση αναλωσίμων (φιαλίδια, σύριγγες, κλπ)
- Μείωση χρόνου παραδόσεως αποτελεσμάτων
- Μείωση λαθών στα αποτελέσματα (άλλου ασθενούς σε άλλον)
- Αύξηση ακρίβειας και αξιοπιστίας αποτελεσμάτων
- Μείωση του όγκου του αρχείου του Νοσοκομείου
- Μείωση του χρόνου ανευρέσεως παλιών αποτελεσμάτων
- Μείωση του κόστους συντηρήσεως των οργάνων
- Γενική οργάνωση των εργαστηρίων
- Ύπαρξη στατιστικών στοιχείων για εκτιμήσεις επενδύσεων ή προμηθειών αναλωσίμων

Υποσυστήματα αποτελούν το ολοκληρωμένο πληροφοριακό εργαστηριακό σύστημα. Το κάθε υποσύστημα του ιατρικού εργαστηρίου έχει τη δυνατότητα να διασυνδέεται τόσο με άλλα πληροφοριακά υποσυστήματα κλινικών, εξωτερικών ιατρείων κλπ ανταλλάσσοντας δεδομένα, όσο και με πληροφοριακά συστήματα τα οποία βρίσκονται εκτός νοσοκομείου. Όλα αυτά, βέβαια, προϋποθέτουν την αυτόματη ενημέρωση του ιατρικού φακέλου του ασθενούς. Για

παράδειγμα, το πληροφοριακό σύστημα απεικονιστικού εργαστηρίου (ακτινολογικό, αξονικός ή μαγνητικός τομογράφος, υπέρηχοι) έχει τη δυνατότητα αποθήκευσης των εικόνων που προέρχονται από τα απεικονιστικά ιατρικά μηχανήματα στη Βάση Δεδομένων (image database). Με την ύπαρξη πληροφοριακού συστήματος, την αρχειοθετημένη εικόνα μπορούν και την βλέπουν τόσο οι εργαστηριακοί ιατροί ιδιωτικών κέντρων όσο και εργαστηριακοί ιατροί νοσοκομειακών ιδρυμάτων.

Ένα από τα υποσυστήματα του εργαστηριακού πληροφοριακού συστήματος αποτελεί το πληροφοριακό σύστημα αιμοδοσίας. Σκοπός της εφαρμογής του συστήματος αιμοδοσίας είναι η πλήρης διαχείριση όλων των εργασιών του τμήματος, καθώς επίσης και της ενσωμάτωσης όλων των χρησιμοποιούμενων διαγνωστικών συσκευών στο πληροφοριακό σύστημα. Ακολουθώντας τη δομή το πληροφοριακού εργαστηριακού συστήματος και το υποσύστημα αυτό είναι δομημένο με τη συλλογιστική πολλαπλών χρηστών. Αποτελείται από ένα δίκτυο υπολογιστών, που «απλώνεται» στο τμήμα της αιμοδοσίας και το οποίο παρέχει πλήρη δυνατότητα διασύνδεσης με το ενιαίο πληροφοριακό σύστημα ή με τις διάφορες κλινικές και τα εργαστήρια, σε κατάσταση πραγματικού χρόνου. Βασικός ρόλος του είναι να διαχειρίζεται πλήρως το ιστορικό των εξετάσεων όλων των ασθενών και αιμοδοτών. Ακόμη, εμφανίζει όλες τις εργαστηριακές εξετάσεις που έχουν πραγματοποιηθεί, τις χορηγημένες μονάδες, τις καλύψεις που έχουν γίνει είτε είναι από αιμοδότες είτε από άλλα νοσοκομεία και τέλος τις διασταυρωμένες μονάδες που υπάρχουν προς χορήγηση. Οι διαδικασίες αυτές αυτοματοποιούνται και η πρόσβαση σε αυτά τα στοιχεία γίνεται άμεσα. Παράλληλα το τμήμα διακίνησης εύκολα και γρήγορα μπορεί να έχει όλες τις πληροφορίες που του χρειάζονται όπως ποιά και πόσα είναι τα αποθέματα μονάδων, ποιές μονάδες υπάρχουν προς χορήγηση εσωτερικών ασθενών, τα υπόλοιπα των ασθενών που έχουν προκύψει από χορηγήσεις μονάδων και αιτήσεις καλύψεων καθώς επίσης και τις εκκρεμότητες που υπάρχουν για επικοινωνία με αιμοδοσίες άλλων νοσοκομείων. Παράλληλα δίνεται η δυνατότητα εκτύπωσης όλων των καταστάσεων και κινήσεων που είναι υποχρεωτικές, με αποτέλεσμα να καταργούνται όλα τα βιβλία που χωρίς το πληροφοριακό εργαστηριακό σύστημα αιμοδοσίας είναι απαραίτητο να κρατούνται χειρόγραφα. Αποθέματα μονάδων, λογιστικό έλλειμμα μονάδων ασθενών, στατιστική κίνηση μονάδων ανά κλινική και ιατρό, εισαγωγές μονάδων από άλλα νοσοκομεία, ειδοποιήσεις αιμοδοτών, απαλλάσσουν το προσωπικό από απαραίτητες μεν, χρονοβόρες δε, εργασίες παρέχοντας με ασφάλεια και αξιοπιστία όλες τις απαραίτητες πληροφορίες. Ουσιαστική μπορεί, λοιπόν, να θεωρηθεί η ύπαρξη και η χρήση του πληροφοριακού εργαστηριακού συστήματος αιμοδοσίας.

Συμπερασματικά, η διαχείριση της πληροφορίας γίνεται στιβαρή με ελαχιστοποίηση λαθών, με υποδιπλασιασμό σχεδόν του απαιτούμενου χρόνου, με δραστική μείωση του αριθμού των επανεξετάσεων μέσω ενσωματωμένου συστήματος ελέγχου ποιότητας και συνεπώς ουσιαστική μείωση του κόστους παραγωγής, τόσον από πλευράς αναλώσιμων υλικών όσο και από

πλευράς χρόνου απασχόλησης προσωπικού. Ο συνδυασμός της μείωσης του κόστους και της αύξησης της αξιοπιστίας των μετρήσεων που παρέχει ένα ολοκληρωμένο πληροφοριακό σύστημα εργαστηρίων, είναι προφανές ότι έχει τεράστια και ουσιαστικότατα οφέλη.

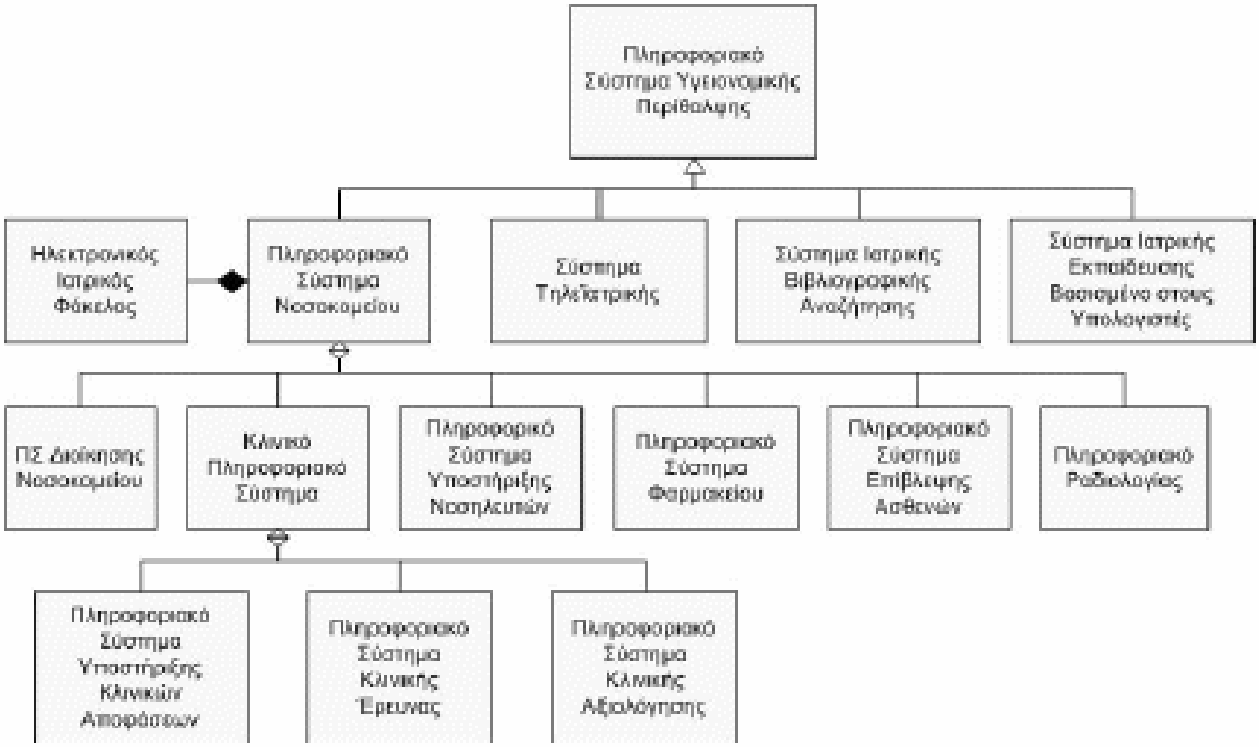
1.4.4 Νοσοκομειακά Πληροφοριακά Συστήματα

Τα πληροφοριακά συστήματα νοσοκομείου είναι μεγάλα, περίπλοκα συστήματα υπολογιστών που έχουν σχεδιαστεί για να βοηθούν στην επικοινωνία και στη διαχείριση των αναγκών πληροφόρησης ενός νοσοκομείου. Αποτελούν εργαλεία για ενδοτομεακή και διατομεακή χρήση. Ένα πληροφοριακό σύστημα νοσοκομείου έχει εφαρμογή σε θέματα εισαγωγής ασθενών, σε ιατρικά αρχεία, σε λογιστικές πληροφορίες, επιχειρησιακές υπηρεσίες, νοσηλευτική, εργαστήρια, ακτινολογικό, φαρμακείο, κεντρικές προμήθειες, διαιτολογικές υπηρεσίες, προσωπικό και μισθοδοσία. Πολλές άλλες εφαρμογές μπορούν να υπάρξουν για κάθε τμήμα και ουσιαστικά για κάθε σκοπό.

Οι εφαρμογές που αφορούν την εισαγωγή ασθενών περιλαμβάνουν προγραμματισμό ασθενών, προεισαγωγική φάση, φάση εισαγωγής, φάση εξόδου από το νοσοκομείο, μεταφορές και διαδικασίες καταγραφής. Ορισμένες εφαρμογές που αφορούν ιατρικά αρχεία περιλαμβάνουν την τήρηση γενικού μητρώου ασθενών, έγγραφα, αλληλογραφία και διαδικασίες εντοπισμού ιατρικών αρχείων. Οι επιχειρησιακές και λογιστικές διαδικασίες περιλαμβάνουν επιβεβαίωση ασφάλειας ασθενούς, χρέωση παρεχομένων υπηρεσιών, παρακολούθηση μετά τη χρέωση, επίλυση αποριών όσον αφορά τις χρεώσεις, λογαριασμούς πληρωτέους, λογαριασμούς εισπρακτέους, διαχείριση μετρητών και τήρηση αρχείου υπηρεσιών και τρίτων φορέων.

Οι εφαρμογές σε άλλους τομείς όπως η νοσηλευτική, τα εργαστήρια, το ακτινολογικό, το φαρμακείο και το τμήμα κεντρικών προμηθειών μπορεί να είναι πολλές και περίπλοκες και να διαθέτουν δικά τους πληροφοριακά συστήματα. Τα συστήματα αυτά ξεχωρίζουν και λειτουργούν ανεξάρτητα από το πληροφοριακό σύστημα του νοσοκομείου, αλλά συνήθως συνδέονται μεταξύ τους για τη μεταβίβαση πληροφοριών.

Όπως τονίζει ο Hasselbring (1999) ο όρος πληροφοριακό σύστημα νοσοκομείου αναφέρεται στο ίδρυμα σαν σύνολο, το οποίο περιλαμβάνει τόσο τις λειτουργίες των κλινικών, όσο και αυτές των διοικητικών και οικονομικών τμημάτων αλλά και τις λειτουργίες των εργαστηρίων, του φαρμακείου, κτλ. Το κλινικό πληροφοριακό σύστημα και το πληροφοριακό σύστημα διαχείρισης αποτελούν υποσυστήματα του πληροφοριακού συστήματος του νοσοκομείου. Στο σχήμα φαίνεται μία ταξινόμηση των πληροφοριακών συστημάτων υγείας, όπως αυτή προτείνεται από τον Hasselbring.



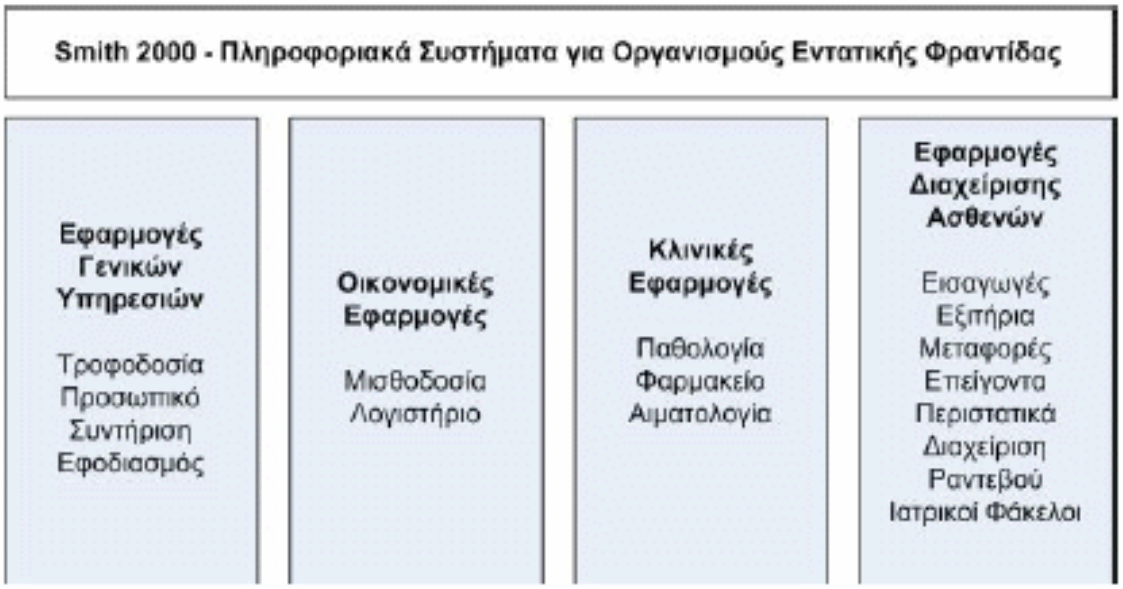
Σχήμα 1.1 *Παράδειγμα ταξινόμησης για τα πληροφοριακά συστήματα υγείας (προσαρμοσμένο από Hasselbring, 1999)*

Η ταξινόμηση αυτή του Hassebring δεν είναι μοναδική. Ο Zviran το 1990 διαχωρίζει τις εφαρμογές ενός Π.Σ.Ν. σε 4 υπό-ομάδες εφαρμογών που σύμφωνα με αυτόν καλύπτουν όλες τις απαιτήσεις ενός πληροφοριακού συστήματος νοσοκομείου. Αυτές είναι:

- Διοίκηση (Λογιστικά, χρηματοοικονομικά, εξοπλισμός, αποθήκες, γενική διοίκηση)
- Διαχείριση Ασθενών (Εισαγωγές, Ιατρικός φάκελος, Κλινικές εφαρμογές, Παρακολούθηση)
- Διαχείριση Υπηρεσιών (Εργαστηριακές εφαρμογές, Χειρουργεία, Τράπεζα αίματος, Φαρμακείο, Ραδιολογία)
- Ιατρικές Εφαρμογές. (Υποστηρικτικές διαγνώσεις, Ιατρικές Αναφορές, Ιατρική έρευνα)

Σχήμα 1.2 *Πληροφοριακό σύστημα νοσοκομείου σύμφωνα με τον Zviran 1990 (πηγή Smith 2000 σελ. 201)*

Ο Smith (2000) αναφέρει πως, στις μέρες μας η παραδοσιακή έννοια του νοσοκομείου έχει διευρυνθεί σε αυτό που ονομάζει, οργανισμούς εντατικής φροντίδας (acute health care organizations). Τα πληροφοριακά συστήματα που αναπτύσσονται για τους οργανισμούς αυτούς έχουν πολλά κοινά με τα πληροφοριακά συστήματα που αναπτύσσονται για ξενοδοχεία ή αεροπορικές εταιρίες, με την έννοια ότι έχουν ένα κεντρικό κατάλογο στον οποίο αναφέρονται οι περισσότερες εφαρμογές. Στην περίπτωση των νοσοκομείων, ο κατάλογος αυτός είναι ο κατάλογος των ασθενών. Ο Smith (2000) κατατάσσει τις εφαρμογές των πληροφοριακών συστημάτων που χρησιμοποιούνται στους «οργανισμούς εντατικής φροντίδας» σε 4 κατηγορίες (σχήμα 1-3).



Σχήμα 1.3 *Πληροφοριακά συστήματα για οργανισμούς εντατικής φροντίδας σύμφωνα με τον Smith*

Ο Smith (2000) εξετάζει τα πληροφοριακά συστήματα σαν εργαλεία που χρησιμοποιούνται για την διαχείριση των λειτουργιών σε έναν οργανισμό (management information systems). Υπό αυτή την οπτική μπορούμε να διακρίνουμε διάφορα υποσυστήματα του ΠΣΝ ανάλογα με τις διαχειριστικές λειτουργίες που υποστηρίζουν. Έτσι για ένα πληροφοριακό σύστημα νοσοκομείου, έχουμε (Smith 2000):

- Διαχείριση Λειτουργιών Νοσοκομείου
- Διαχείριση Οικονομικών και Ανθρώπινων Πόρων
- Ιατρική και διοικητική διαχείριση ασθενών
- Διαχείριση αποθηκών
- Διαχείριση πόρων

Στην ελληνική βιβλιογραφία σε μία μελέτη που εκπονήθηκε από την «01-Πληροφορική Α.Ε.» για λογαριασμό του Υπουργείου Υγείας το 1998, αναφέρεται ότι τα πληροφοριακά υποσυστήματα που συγκροτούν ένα ολοκληρωμένο πληροφοριακό σύστημα νοσοκομείου (Ο.Π.Ν.Σ.) διακρίνονται στα ακόλουθα υποσυστήματα:

Α. Το διαχειριστικό / οικονομικό: Περιλαμβάνει τις λειτουργίες διαχειριστικής και οικονομικής οργάνωσης.

1. Διαχειριστικές λειτουργίες:

a. Διαχείριση ασθενών

- Νοσηλευομένων (Γραφείο Κίνησης)
- Εξωτερικών ασθενών (Γραμματεία Εξωτερικών Ιατρείων)

- Επειγόντων περιστατικών (Τμήμα Επειγόντων Περιστατικών)

b. Διαχείριση προσωπικού

c. Διαχείριση υλικών

d. Διαχείριση προμηθειών

e. Διαχείριση εγκαταστάσεων

f. Τιμολόγηση παρεχόμενων υπηρεσιών (νοσηλείας, ιατρικών πράξεων, εργαστηριακών εξετάσεων, χρήσης υλικών και φαρμάκων)

2. Οικονομικές Λειτουργίες:

a. Γενική Λογιστική

b. Αναλυτική Λογιστική

c. Ταμειακός προγραμματισμός

d. Προϋπολογισμός

e. Λογιστήριο ασθενών

f. Εκκαθάριση ασφαλιστικών ταμείων

g. Διαχείριση παραμέτρων νοσηλίων

h. Εισπράξεις / Πληρωμές

i. Διαχείριση Παγίων

j. Μισθοδοσία Προσωπικού

Β. Το ιατρικό: Καλύπτει τις ανάγκες διεκπεραίωσης των εργασιών που επιτελούνται στα κλινικά τμήματα του νοσοκομείου (Παπουτσής 1999). Περιλαμβάνει:

1. Εφαρμογές παροχής ιατρικής φροντίδας, υποστηρίζουν το κλινικό τμήμα στην υλοποίηση της καθαρά ιατρικής φροντίδας που παρέχεται στον ασθενή κατά την διάρκεια της νοσηλείας του. Περιλαμβάνει:

a. Διαχείριση ασθενή (εισαγωγή, έξοδος, μετακίνηση ασθενούς)

b. Διαχείριση ιστορικού ασθενούς

c. Παρακολούθηση πορείας υγείας (συμπτώματα ασθενή, κλινικά σημεία,

διαγνώσεις, πορεία νόσου)

d. Διαχείριση ιατρικών εντολών και παρουσίαση αποτελεσμάτων

Ανάλογα με την ιατρική εξειδίκευση του κλινικού τμήματος (Καρδιολογικό, Χειρουργικό, Νεφρολογικό, Ογκολογικό κτλ.) υπάρχουν πρόσθετες απαιτήσεις πληροφοριακής υποστήριξης οι οποίες ενσωματώνονται στις λειτουργίες του υποσυστήματος ιατρικής φροντίδας.

2. Εφαρμογές παροχής νοσηλευτικής φροντίδας. Υποστηρίζουν το νοσηλευτικό προσωπικό στην διαχείριση του νοσηλευτικού έργου. Περιλαμβάνουν:

a. Σχεδιασμός νοσηλευτικής φροντίδας

b. Νοσηλευτική παρακολούθηση

c. Νοσηλευτικές ενέργειες και πράξεις

d. Φαρμακολογική παρακολούθηση ασθενούς

3. Παράλληλες υποστηρικτικές εφαρμογές.

a. Νοσοκομειακό Φαρμακείο

b. Προγραμματισμός ιατρικού και νοσηλευτικού προσωπικού

c. Διαχείριση τακτικών εξωτερικών ιατρείων

d. Προγραμματισμός χειρουργείων

e. Διαιτολογικό

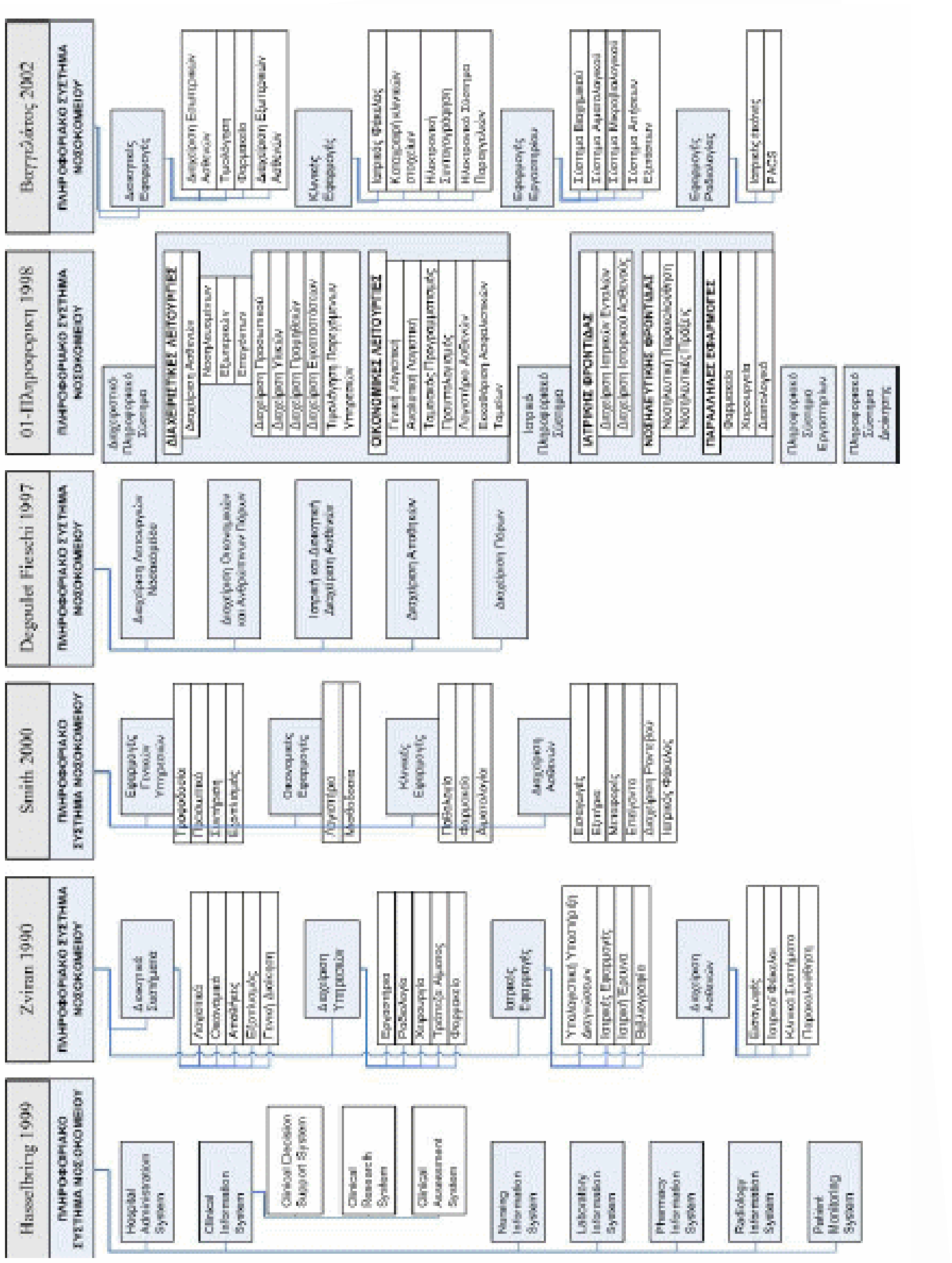
Γ. Το εργαστηριακό: Εξειδικευμένα συστήματα τα οποία επιτρέπουν την σύνδεση των σύγχρονων αναλυτικών συσκευών με το διαχειριστικό σύστημα του εκάστοτε εργαστηρίου. Για τα απεικονιστικά εργαστήρια, έχουν αναπτυχθεί ανάλογα συστήματα με τα οποία επιτυγχάνεται η σύνδεση των απεικονιστικών μηχανημάτων με το διαχειριστικό σύστημα του εργαστηρίου (Radiology Information Systems, RIS). Παράλληλα έχουν αναπτυχθεί εξειδικευμένα συστήματα για την αποθήκευση, ανάκληση και μεταφορά της ιατρικής εικόνας (Picture Archiving and Communications Systems, P.A.C.S.) εντός του νοσοκομείου. (Βαγγελάτος 2002)

Δ. Πληροφοριακό Σύστημα Διοίκησης (ΠΣΔ): Παρέχει την δυνατότητα συγκέντρωσης στοιχείων από όλες τις δραστηριότητες του οργανισμού, ώστε μέσα από την κατάλληλη σύνδεσή τους να προκύψουν οι δείκτες εκείνοι που θα αξιολογήσουν τις δραστηριότητες αυτές και θα βοηθήσουν το διοικητικό μηχανισμό στην λήψη αποφάσεων. Το ΠΣΔ αντλεί πληροφορίες από όλα τα υποσυστήματα του νοσοκομείου και τις παρουσιάζει με κατανοητό και επεξεργάσιμο τρόπο στην διοίκηση του οργανισμού. Τα δεδομένα τα οποία χρειάζεται κατ' ελάχιστον ένα ΠΣΔ είναι ενδεικτικά τα εξής: κοστολογικά δεδομένα, δεδομένα προσωπικού και μισθολογικά δεδομένα, ιατρικές πράξεις στις οποίες υποβάλλονται οι ασθενείς, διαγνώσεις. (Βαγγελάτος 2002)

Σε έρευνα που εκπονήθηκε από το 2001 από τον Ινστιτούτο Τεχνολογίας Υπολογιστών (Ι.Τ.Υ) (Βαγγελάτος, 2002) οι εφαρμογές των πληροφοριακών συστημάτων νοσοκομείων χωρίστηκαν στις ακόλουθες 4 κατηγορίες:

- Διοικητικές Εφαρμογές (Administration System)
- Κλινικές Εφαρμογές (Clinical System)
- Εφαρμογές Εργαστηρίου (Laboratory System)
- Εφαρμογές Ραδιολογίας (Radiology System)

Στο σχήμα 1.4 φαίνονται συγκεντρωτικά όλα τα μοντέλα που παρουσιάστηκαν σε αυτήν την παράγραφο. Παρατηρούμε ότι επικρατεί ασυμφωνία όσον αφορά στο καταλληλότερο μοντέλο για την περιγραφή ενός πληροφοριακού συστήματος νοσοκομείου. Ο Α. Βαγγελάτος (2002) υποστηρίζει ότι το ενδιαφέρον δεν πρέπει να εστιάζεται τόσο στο διαχωρισμό και την ονοματολογία των υποσυστημάτων όσο στην πληρότητα όλων των υποστηρικτικών εφαρμογών για την καλύτερη δυνατή λειτουργία του νοσοκομείου. Ωστόσο, στον αντίποδα, υποστηρίζεται ότι η συστηματική ταξινόμηση και η χρήση ακριβούς ορολογίας είναι πολύ σημαντικά βήματα στην επίλυση προβλημάτων που προέρχονται από την σύγχυση και την ασάφεια στον τομέα αυτό. (Hasselbring 1999)



Σχήμα 1.4 *Συγκεντρωτική επισκόπηση των διαφόρων δομών των νοσοκομειακών πληροφοριακών συστημάτων*

1.5 Αρχιτεκτονική Πληροφοριακών Συστημάτων Νοσοκομείων

Τα πρώτα συστήματα που τοποθετήθηκαν την δεκαετία του 70 [Collen 1974], χαρακτηρίζονταν από αρχιτεκτονική κεντρική, που αποτελούνταν από ένα κεντρικό υπολογιστή και περιφερειακά συνδεδεμένα σε αστέρα [Peterson 1988]. Σε αρχιτεκτονικές τέτοιου τύπου ένας κεντρικός υπολογιστής διαχειρίζεται όλη την πληροφορία και τα τερματικά και οι εκτυπωτές που χρησιμοποιούνται για την ανταλλαγή πληροφορίας.

Όπως αναφέρεται από τον Junghans (1995) η ανάγκη για αποκεντροποίηση των πληροφοριακών δικτύων δεν προέκυψε σαν μία απαίτηση για την ανάπτυξη του ίδιου του δικτύου, αλλά από την δομή των λειτουργικών μονάδων μέσα στο νοσοκομείο. Τα διάφορα σημεία όπου εργάζεται το προσωπικό είναι διάσπαρτα μέσα στον χώρο του νοσοκομείου και έτσι πρέπει και οι σταθμοί εργασία να κατανέμονται αντίστοιχα. (Mulligen 1992)

Πρέπει επίσης να έχουμε υπόψη μας πως σχεδόν πάντα ένα ΝΠΣ δομείται πάνω σε προϋπάρχοντα υποσυστήματα που λειτουργούν για συγκεκριμένες ιατρικές ή διοικητικές λειτουργίες. (Prokosch 1995)

Από την ανάγκη για συνένωση των επιμέρους υπολογιστικών συστημάτων προέκυψαν τα κατανεμημένα δίκτυα. Αυτά υλοποιούνται από ένα σύνολο τοπικών δικτύων (LAN) όπου υπάρχουν διάφοροι υπολογιστές που είναι δομημένοι έτσι ώστε να υλοποιούν συγκεκριμένες λειτουργίες.

Τα κατανεμημένα δίκτυα παρέχουν απευθείας υποστήριξη σε αποκεντρωμένες μονάδες. Τα τοπικά δίκτυα κάνουν χρήση της δικιάς τους δυνατότητας επεξεργασίας ενώ παράλληλα τους δίνεται η δυνατότητα πρόσβασης σε πληροφορίες που προέρχονται και αφορούν το σύνολο του οργανισμού. Με αυτή την αρχιτεκτονική μεγιστοποιείται η χρήση δικτυακών πόρων, υπηρεσιών και βάσεων δεδομένων. Ένα από τα βασικά τους πλεονεκτήματα είναι ότι υπάρχει η δυνατότητα ενσωμάτωσης νέων εφαρμογών που μπορεί να προέρχονται από διαφορετικές πηγές. (Scherer 1995) Έτσι εξασφαλίζεται η συνεχής εξέλιξη και ανάπτυξη του συνολικού πληροφοριακού δικτύου.

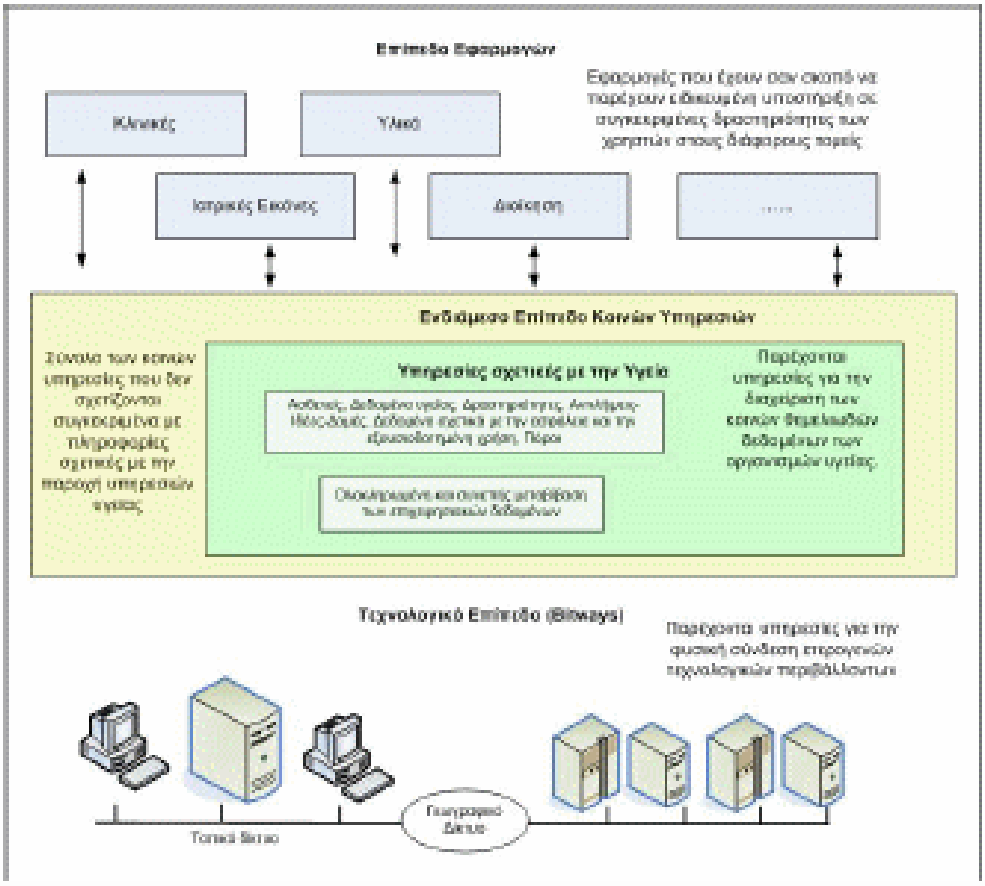
Μία από τις μεγαλύτερες προκλήσεις στον χώρο των πληροφοριακών συστημάτων των νοσοκομείων είναι η ολοκλήρωση ενός συνόλου ανεξάρτητων δικτύων σε ένα κατανεμημένο σύνολο που να παρουσιάζει συνοχή και να επιτρέπει την συνεργασία των διάφορων εφαρμογών προς την επίτευξη των κοινών στόχων που θέτονται μέσα στο ευρύτερο νοσοκομειακό περιβάλλον.

Ένα ακόμα μεγάλο ερώτημα είναι το πώς θα πρέπει να είναι μορφοποιημένα αυτά τα κατανεμημένα δίκτυα ώστε να μπορεί να επιτυγχάνεται ταυτόχρονα, τόσο η προσαρμογή του κάθε δικτύου στις ιδιαίτερες απαιτήσεις του κάθε οργανισμού όσο και η εφαρμογή κοινών

προτύπων στην ανάπτυξη των δικτύων που θα διευκολύνουν τόσο την ανάπτυξη των επιμέρους εφαρμογών όσο και την επικοινωνία μεταξύ των υποσυστημάτων τόσο σε επίπεδο εφαρμογής όσο και σε επίπεδο οργανισμών.

Σαν απάντηση στην τεχνολογική διασύνδεση των κατανεμημένων συστημάτων προτείνονται στοιχεία ενδιάμεσου επιπέδου (middleware). Η προσέγγιση αυτή θεωρεί πως ένας οργανισμός υγείας (όπως ένα νοσοκομείο) είναι ένα σύνολο ανόμοιων χρηστών, που εκτελούν ποικίλες δραστηριότητες αλλά που έχουν την απαίτηση να βασίζονται και να μοιράζονται ένα κοινό σύνολο δεδομένων και να χρησιμοποιούν ένα κοινό σύνολο υπηρεσιών. (Grimson 2000).

Το CEN ENV 12967–1 (HISA) είναι ένα πρότυπο που προωθείται από την Ευρωπαϊκή Επιτροπή Προτυποποίησης (CEN), που αγκαλιάζει την ιδέα αυτή του ενδιάμεσου επιπέδου. Το πληροφοριακό μοντέλο που προτείνεται αποτελείται από τρία επίπεδα που συνεργάζονται μεταξύ τους: τις εφαρμογές, το ενδιάμεσο επίπεδο και τα bitways. Κάθε ένα από αυτά τα επίπεδα είναι ξεχωριστά υπεύθυνο να καλύπτει συγκεκριμένες πλευρές του σχεδιασμού και τις λειτουργικότητας του πληροφοριακού συστήματος. Τα τρία επίπεδα παριστάνονται γραφικά στο σχήμα.

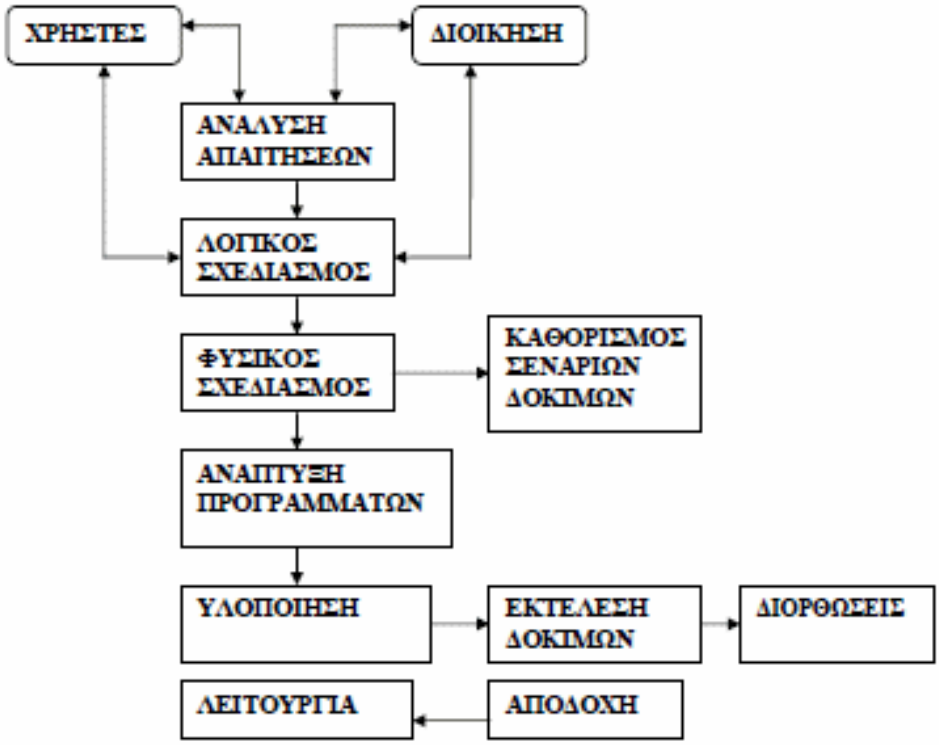


Σχήμα 1.5 *Τα τρία επίπεδα του προτύπου H.I.S.A. (προσαρμοσμένο από: Grimson 2000)*

Επιπλέον σημαντικά πρότυπα που στοχεύουν στην επίτευξη της διασυνδεσιμότητας των εφαρμογών και φαίνεται να κερδίζουν έδαφος στον χώρο της ανάπτυξης συστημάτων υγείας είναι αυτά που προκύπτουν από τον οργανισμό προτυποποίησης HL7, και στα οποία θα γίνει εκτενέστερη αναφορά στο επόμενο κεφάλαιο. Εν συντομία, οι κανόνες που συνθέτουν τα πρότυπα αυτά, αποσκοπούν στον καθορισμό του τρόπου με τον οποίο επικοινωνούν τα διάφορα συστήματα ή ιατρικά μηχανήματα μεταξύ τους. Στόχος είναι να εξασφαλίζεται η επικοινωνία μεταξύ όλων αυτών των διαφορετικών τμημάτων ανεξάρτητα από τον κατασκευαστή ή την τεχνολογία κατασκευής του κάθε υποσυστήματος. Από το 2003 ιδρύθηκε και λειτουργεί στην Ελλάδα, το ελληνικό τμήμα του οργανισμού HL7. Πέρα από την προώθηση της χρήσης και αποδοχής των προτύπων HL7 στην Ελλάδα, το τμήμα αυτό είναι επιφορτισμένο με την τεχνική προσαρμογή των προτύπων του HL7 στις απαιτήσεις του ελληνικού χώρου. Απώτερος στόχος είναι η δημιουργία Εθνικών οδηγών υλοποίησης ώστε να τεθούν οι βάσεις για την μείωση των λαθών και την αποτελεσματικότερη παροχή υπηρεσιών υγείας, ενώ ταυτόχρονα να βελτιωθεί η ανταγωνιστικότητα των εταιριών που δραστηριοποιούνται στο χώρο της ιατρικής πληροφορικής στην Ελλάδα.

1.6 Κύκλος Ζωής Πληροφοριακών Συστημάτων Υγείας

Ο κύκλος ζωής πληροφοριακών συστημάτων υγείας περιλαμβάνει τις φάσεις που απαιτούνται για την ανάπτυξη, λειτουργία και συντήρηση τους. Σε κάθε φάση εκτελούνται συγκεκριμένες εργασίες σε συγκεκριμένο χρόνο και με τη χρήση των απαιτούμενων πόρων. Επίσης, από κάθε φάση παράγονται συγκεκριμένα αποτελέσματα, τα οποία πρέπει να τεκμηριώνονται επαρκώς. Ένας τυπικός κύκλος ζωής πληροφοριακών συστημάτων αποτελείται από έξι φάσεις: την ανάλυση απαιτήσεων, το λογικό σχεδιασμό, το φυσικό σχεδιασμό, την ανάπτυξη προγραμμάτων, την υλοποίηση και τη λειτουργία. Η σχέση των φάσεων αυτών φαίνεται στο ακόλουθο σχήμα.



Σχήμα 1.6 *Κύκλος ζωής πληροφοριακού συστήματος υγείας*

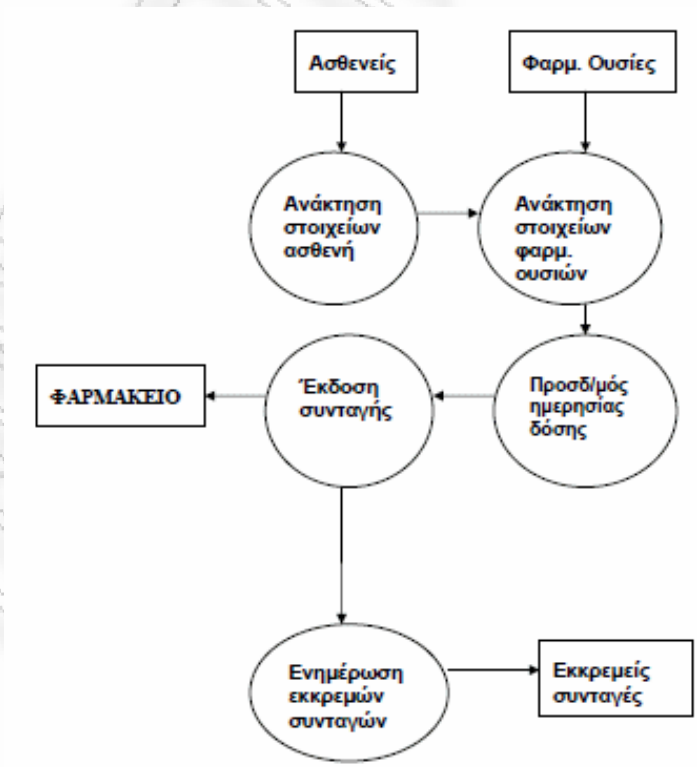
Ανάλυση απαιτήσεων: Η πρώτη φάση του κύκλου ζωής αφορά τον προσδιορισμό των απαιτήσεων του πληροφοριακού συστήματος υγείας. Συγκεκριμένα, κατά τη φάση αυτή γίνονται επαναλαμβανόμενες συναντήσεις μεταξύ των αναλυτών του συστήματος και των υπευθύνων του οργανισμού έτσι ώστε να προσδιοριστεί σαφώς το πλαίσιο του συστήματος και οι δυνατότητες επικοινωνίας του με άλλα συστήματα. Τα αποτελέσματα των συναντήσεων αυτών μελετώνται από τους αναλυτές, οι οποίοι στη συνέχεια υποβάλλουν στον οργανισμό την πρόταση τους στην οποία δίνεται η περιγραφή του συστήματος, οι απαιτούμενοι πόροι, ο αναμενόμενος χρόνος υλοποίησης του καθώς και το κόστος του. Στη συνέχεια, και μετά την αποδοχή της πρότασης από τους υπεύθυνους του οργανισμού, εκτελούνται οι ακόλουθες εργασίες: μελέτη της τρέχουσας λειτουργίας του οργανισμού, καταγραφή εναλλακτικών λύσεων, αξιολόγηση και επιλογή της καταλληλότερης λύσης. Με βάση τις πληροφορίες αυτές κατασκευάζεται το μοντέλο λειτουργίας του νοσοκομείου το οποίο δίνει τη δυνατότητα ολοκληρωμένης και λεπτομερούς θεώρησης και μελέτης του.

Μετά την επιλογή της καταλληλότερης λύσης από τον οργανισμό, προετοιμάζεται το πρόγραμμα έργου το οποίο περιλαμβάνει τους στόχους του, τις εργασίες που θα εκτελεστούν, τα χρονικά σημεία στα οποία περατώνεται η εκτέλεση ενός συνόλου εργασιών ή ξεκινά η έναρξη ενός άλλου και γίνεται ο έλεγχος της επίτευξης των στόχων. Ο έλεγχος αυτός περιλαμβάνει τη σύγκριση του

προϋπολογιζόμενου και του πραγματικού κόστους, καθώς και την ανασκόπηση της ποιότητας της εργασίας που έχει εκτελεστεί.

Λογικός σχεδιασμός: Κατά τη φάση αυτή καθορίζεται λογικά η δομή του πληροφοριακού συστήματος υγείας. Συγκεκριμένα, οι πληροφοριακές απαιτήσεις του οργανισμού μετασχηματίζονται σε ένα εννοιολογικό μοντέλο του νέου συστήματος. Για την κατασκευή του μοντέλου αυτού μπορεί να χρησιμοποιηθούν διάφορες τεχνικές, όπως τα διαγράμματα ροής δεδομένων, το λεξικό δεδομένων, τα διαγράμματα δομών δεδομένων, οι πίνακες αποφάσεων κ.λπ.

Συγκεκριμένα, τα διαγράμματα ροής δεδομένων είναι μία από τις πιο γνωστές μεθόδους ανάλυσης και σχεδιασμού ενός πληροφοριακού συστήματος. Χρησιμοποιώντας τη μέθοδο αυτή μπορούμε να περιγράψουμε την τρέχουσα λειτουργία ενός συστήματος, αναπαριστώντας τα επιμέρους συστατικά του σε οποιοδήποτε επιθυμητό επίπεδο λειτουργίας. Έτσι, μέσω διαγραμμάτων ροής δεδομένων σχηματίζουμε μία παραστατική εικόνα μέσω της οποίας μπορούμε να σχεδιάσουμε τις προτεινόμενες λύσεις. Στο παρακάτω σχήμα παρουσιάζεται το διάγραμμα ροής δεδομένων της διαδικασίας «Συνταγογράφησης».



Σχήμα 1.7 *Διάγραμμα ροής δεδομένων της διαδικασίας "Συνταγογράφησης"*

Λεξικό δεδομένων ονομάζεται το σύνολο των πληροφοριών σχετικά με τα δεδομένα που χρησιμοποιεί ή προβλέπεται ότι θα χρησιμοποιήσει το πληροφοριακό σύστημα. Οι πληροφορίες που περιλαμβάνει αφορούν το όνομα, την κατηγορία του, τη χρήση του, τον τρόπο διαχείρισης του κ.λπ. Τα διαγράμματα δομών χρησιμοποιούνται για τη λειτουργική διάσπαση ενός συστήματος σε υποσυστήματα και είναι ιδιαίτερα χρήσιμα σε συστήματα μεγάλου μεγέθους. Πίνακας αποφάσεων ονομάζεται ένας πίνακας στον οποίο καταγράφονται οι λειτουργικοί κανόνες ενός οργανισμού με τη μορφή συνθηκών και ενεργειών.

Από τη κατασκευή των μοντέλων αυτών καταγράφονται συμπεράσματα τα οποία αφορούν:

- Τα κύρια συστατικά υποσυστήματα του οργανισμού και τους τρόπους επικοινωνίας μεταξύ τους ή και με συστήματα άλλων οργανισμών,
- Τις εργασίες που εκτελούνται σε καθένα από τα υποσυστήματα, καθώς και τον τρόπο εκτέλεσης τους,
- Τη ροή δεδομένων από τη πηγή μέχρι και τη διάθεση τους στους τελικούς χρήστες,
- Τις επεξεργασίες και τους μετασχηματισμούς των δεδομένων από την εκτέλεση των εργασιών,
- Τα είδη των αρχείων που χρησιμοποιούνται για την αποθήκευση των δεδομένων και
- Τις απαιτήσεις σε πόρους (ανθρώπινους, υλικούς και χρηματικούς) για την εκτέλεση των εργασιών.

Φυσικός σχεδιασμός: Κατά τη φάση αυτή γίνεται ο σαφής καθορισμός των υποσυστημάτων, της βάσης δεδομένων και των προγραμμάτων εφαρμογών του πληροφοριακού συστήματος. Τη βάση για τον καθορισμό αυτό αποτελούν τα συμπεράσματα του λογικού σχεδιασμού. Συνήθως, χρησιμοποιούνται μέθοδοι για το σχεδιασμό των λογικών τμημάτων στο λογισμικό των εφαρμογών του πληροφοριακού συστήματος, όπως είναι τα διαγράμματα δομής δεδομένων.

Ο σχεδιασμός της βάσης δεδομένων αφορά τη λογική και φυσική δόμηση των δεδομένων και τον καθορισμό των μεθόδων προσπέλασης τους. Συγκεκριμένα, ο σχεδιασμός αυτός περιλαμβάνει τον καθορισμό των αρχείων δεδομένων, τις τεχνικές προσπέλασης τους, τα προβλεπόμενα μεγέθη αρχείων δεδομένων και ευρετηρίων, τη διαδικασία λήψης αντιγράφων, τις επιπτώσεις από την αναδιοργάνωση τη βάσης δεδομένων και το σύστημα ασφαλείας της. Τα αποτελέσματα της φάσης αυτής υποβάλλονται στη διοίκηση του οργανισμού για μελέτη και αποδοχή και χρησιμοποιούνται ως βάση για την επόμενη φάση, την ανάπτυξη των προγραμμάτων.

Ανάπτυξη προγραμμάτων: Κατά τη φάση αυτή τα λογικά τμήματα του λογισμικού των εφαρμογών που προσδιορίστηκαν το στάδιο του φυσικού σχεδιασμού υλοποιούνται και ενώνονται μεταξύ τους ενώ παράλληλα υλοποιείται και η βάση δεδομένων του συστήματος. Η συγγραφή των προγραμμάτων εκτελείται από την ομάδα προγραμματιστών του συστήματος και

γίνεται με τη χρήση κάποιας γλώσσας προγραμματισμού (π.χ. c++, Visual Basic κ.λπ.). Σε μεγάλα έργα ανάπτυξης πληροφοριακών συστημάτων η ομάδα των προγραμματιστών διασπάται σε υποομάδες, καθεμία από τις οποίες έχει ένα προϊστάμενο προγραμματιστή , οι οποίες αναλαμβάνουν τη συγγραφή ενός συνόλου εφαρμογών (που συνήθως αφορούν ένα ανεξάρτητο υποσύστημα). Το αποτέλεσμα της φάσης αυτής είναι το ολοκληρωμένο λογισμικό εφαρμογών του πληροφοριακού συστήματος και το αντίστοιχο υποστηρικτικό υλικό.

Υλοποίηση: Κατά τη φάση αυτή γίνεται η δοκιμή του λογισμικού των εφαρμογών, εκπαιδεύονται οι χρήστες και εγκαθίστανται το νέο σύστημα.

Η δοκιμή του λογισμικού αφορά τόσο τη δοκιμή του κώδικα όσο και τον έλεγχο της ικανοποίησης των προδιαγραφών του συστήματος, όπως ορίστηκαν στις προηγούμενες φάσεις. Για τη δοκιμή αυτή δημιουργούνται διάφορα σενάρια εκτέλεσης των εφαρμογών έτσι ώστε να ελεγχθούν όλες οι δυνατές περιπτώσεις. Για παράδειγμα, για τον έλεγχο του κώδικα τα σενάρια αυτά εξασφαλίζουν ότι θα ελεγχθεί η εκτέλεση κάθε γραμμής εντολής που περιλαμβάνει. Η δοκιμή των εφαρμογών γίνεται τόσο στο επίπεδο μονάδας όσο και στο επίπεδο ολοκληρωμένου λογισμικού. Στην πρώτη περίπτωση η κάθε εφαρμογή εξετάζεται ανεξάρτητα από τις άλλες με σκοπό να βρεθούν τυχόν λογικά ή προγραμματιστικά λάθη. Στη δεύτερη περίπτωση η δοκιμή αφορά τον έλεγχο και τον εντοπισμό τυχόν λαθών ως προς την ικανοποίηση των αρχικών προδιαγραφών και την επικοινωνία των εφαρμογών μεταξύ τους. Στο στάδιο αυτό εξετάζεται επίσης και η υλοποίηση της βάσης δεδομένων. Ελέγχεται δηλαδή η δυνατότητα του συστήματος να αντεπεξέλθει στον μέγιστο φόρτο εργασίας, ο χρόνος απόκρισής του καθώς και η δυνατότητα ανάκαμψης του συστήματος μετά από μία βλάβη.

Παράλληλα με τη δοκιμή του συστήματος γίνεται και η εκπαίδευση των τελικών χρηστών. Κάθε χρήστης πρέπει να γνωρίζει τον ακριβή ρόλο του, τον τρόπο χρήσης του συστήματος και τις δυνατότητες που αυτό του παρέχει. Η εκπαίδευση που παρέχεται δεν είναι η ίδια για όλους τους χρήστες. Ανάλογα με την ειδικότητα, τη θέση στην ιεραρχία του οργανισμού και την προβλεπόμενη χρήση, κάθε χρήστης έχει και την κατάλληλη εκπαίδευση.

Τέλος, στη φάση της υλοποίησης του συστήματος περιλαμβάνεται και η μετάβαση στο νέο σύστημα. Γενικά, υπάρχουν τέσσερις προσεγγίσεις μετάβασης : η παράλληλη, η τμηματική, η πιλοτική και η άμεση. Σύμφωνα με την παράλληλη προσέγγιση, το υπάρχον και το νέο πληροφοριακό σύστημα λειτουργούν ταυτόχρονα για ένα χρονικό διάστημα κατά το οποίο συγκρίνονται τα αποτελέσματα τους. Ακολουθώντας την τμηματική προσέγγιση, η λειτουργία του νέου πληροφοριακού συστήματος ξεκινά σε συγκεκριμένα τμήματα του οργανισμού. Μετά την εξασφάλιση της επιτυχίας του, το σύστημα επεκτείνεται για να καλύψει και τη λειτουργία άλλων τμημάτων και στη συνέχεια εγκαθίστανται και σε αυτά. Με την πιλοτική προσέγγιση, το πληροφοριακό σύστημα υγείας υλοποιείται για ένα ή περισσότερα τμήματα του οργανισμού που

είναι αντιπροσωπευτικά της όλης λειτουργίας του. Τέλος, υπάρχει και η άμεση προσέγγιση η οποία θεωρείται συντομότερη όλων. Σύμφωνα με αυτή, το νέο πληροφοριακό σύστημα αντικαθιστά ολοκληρωτικά το παλιό σε ένα συγκεκριμένο χρονικό σημείο. Μία από τις σημαντικότερες προϋποθέσεις της προσέγγισης αυτής είναι ο καλός χρονικός προγραμματισμός.

Λειτουργία: Μετά την υλοποίηση του συστήματος ακολουθεί το στάδιο της λειτουργίας του κατά το οποίο πρέπει να εξασφαλιστεί ότι το σύστημα παρέχει τα αναμενόμενα οφέλη στον οργανισμό. Κατά τη διάρκεια λειτουργίας του συστήματος είναι δυνατόν να βρεθούν λάθη μικρής κλίμακας τα οποία και διορθώνονται αμέσως. Επίσης, είναι δυνατόν να ζητηθεί η βελτίωση των εφαρμογών ή και η ανάπτυξη νέων με σκοπό τη βελτίωση της αποδοτικότητας όλου του συστήματος.

Τα παραδοτέα της φάσης αυτής είναι το τεκμηριωτικό υλικό του συστήματος: το εγχειρίδιο λειτουργίας το οποίο αφορά τον τρόπο λειτουργίας του συστήματος και απευθύνεται στο προσωπικό μηχανογράφησης του οργανισμού, το εγχειρίδιο συντήρησης το οποίο περιέχει τις διαδικασίες συντήρησης του συστήματος και προορίζεται για αναλυτές και προγραμματιστές και το εγχειρίδιο χρήσης το οποίο περιέχει οδηγίες για τον τρόπο χρήσης του συστήματος και αφορά τους τελικούς χρήστες.

1.7 Οφέλη από την υιοθέτηση ΠΣΥ και Παράγοντες αποτυχίας τους

Σύμφωνα με τον Shorbaji (2001) τα πιθανά οφέλη από την επιστροφή της επένδυσης για την υιοθέτηση πληροφοριακών συστημάτων διακρίνονται σε τρείς κατηγορίες οι οποίες είναι:

1. Ποσοτικά οφέλη: Αυτά είναι οικονομικά οφέλη που είναι σαφώς μετρήσιμα και αποδίδονται στη χρήση μιας ιδιαίτερης τεχνολογίας. Παραδείγματος χάριν η χρήση της τεχνολογίας ηλεκτρονικής ανταλλαγής δεδομένων για να διαβιβαστούν τα στοιχεία ιατρικής παρακολούθησης σε πραγματικό χρόνο, ή για να υποβάλει ηλεκτρονικά τις ιατρικές εργαστηριακές εξετάσεις που οδηγεί σε αποταμίευση κόστους και χρόνου εργασίας.

2. Ποιοτικά οφέλη: Αυτά είτε άμεσα είτε έμμεσα αποδίδονται στην τεχνολογία αλλά είναι δυσκολότερα να ποσοτικοποιηθούν. Αυτά τα οφέλη μετριούνται μόνο σε επίπεδο του αντίκτυπου της τεχνολογίας στην απόδοση των συστημάτων και της αποδοτικότητάς τους. Τα ακριβή στοιχεία, η γρήγορη μεταφορά των στοιχείων, η ευρύτερες δυνατότητα πρόσβασης και η σύνδεση των στοιχείων είναι οφέλη που δεν ποσοτικοποιούνται εύκολα.

3. Στρατηγικά οφέλη: Αυτά ουσιαστικά τα οφέλη είναι πιο μακροπρόθεσμα. Για παράδειγμα η συλλογή και η ανάλυση δεδομένων φέρνουν έχουν ως αποτέλεσμα το άμεσο όφελος στην

οργάνωση των πληροφοριών, αλλά μακροπρόθεσμα αυτό το στοιχείο αποτελεί τη βάση για έρευνα και προγραμματισμό.

Ο Wulsin και Dougherty (2008) υπογραμμίζουν τα οφέλη, τα οποία σχετίζονται με την ταχύτητα και ποιότητα παράδοσης της ιατρικής φροντίδας μέσα από τις ηλεκτρονικά αυτοματοποιημένες διαδικασίες στήριξης αποφάσεων. Επιπλέον την αυξημένη ικανότητα τον επαγγελματιών για αναγνώριση σχεδιασμό, πρόβλεψη, έλεγχο και προγραμματισμό παραγόντων που έχουν σχέση με τις επιδημίες, τα φάρμακα κ.α. Την μείωση των ιατρικών λαθών, τη μείωση του κόστους λειτουργίας και του χρόνου εργασίας.

Επίσης ο Richard Heeks (Aziz, 2005) καθορίζει έναν αριθμό ωφελειών από την υιοθέτηση πληροφοριακών συστημάτων, μέσα από μελέτες περιπτώσεων, τα οποία μπορούν να ομαδοποιηθούν και να ταξινομηθούν σε πολλές κατηγορίες. Μια από αυτές την χωρίζει σε δύο επίπεδα:

- Task level benefits: Για παράδειγμα στη βελτίωση του κόστους και της ταχύτητας επεξεργασίας των δεδομένων και
- Health process level benefits: Για παράδειγμα στην ποιότητα και ταχύτητα οργάνωσης και παράδοσης της ιατρικής φροντίδας.

Παράλληλα τα πληροφοριακά συστήματα μπορούν να βελτιώσουν την κατάσταση προσφέροντας ακόμα περισσότερο σε όχι και τόσο ευδιάκριτα πεδία όπως στην βελτίωση των γνώσεων και δεξιοτήτων των επαγγελματιών υγείας.

Πέρα από τα προφανή οφέλη που αποκομίζονται όπως διαπιστώσαμε και παραπάνω από την εφαρμογή των πληροφοριακών συστημάτων τις περισσότερες φορές το μεγαλύτερο και κυριότερο μειονέκτημα που προβάλλεται είναι το αυξημένο κόστος επένδυσης μιας τέτοιας προσπάθειας.

Η υιοθέτηση των πληροφοριακών συστημάτων υγείας είναι ένας δύσκολος στόχος να επιτευχθεί και η διαδικασία οδηγεί συχνά σε μια αποτυχία αντί για επιτυχία. Οι κυριότεροι λόγοι μιας αποτυχημένης ανάπτυξης-υιοθέτησης, μπορούν να προέλθουν από τις δυσκολίες στον καθορισμό των στόχων του συστήματος και στην επιλογή της μη-κατάλληλης τεχνολογίας για την εφαρμογή. Επιπλέον, μπορεί να υπάρξουν προβλήματα όσον αφορά τον υπολογισμό των δαπανών ανάπτυξης ή των οικονομικών επιδράσεων του συστήματος. Η αποτυχία πολλές φορές μπορεί να προκύψει και από τεχνικούς λόγους, για παράδειγμα αποτυχία και προβλήματα στην επεξεργασία των δεδομένων. Ένας άλλος παράγοντας εξίσου σημαντικός είναι η έλλειψη εξειδικευμένων γνώσεων από τους χρήστες για την χρήση των συγκεκριμένων τεχνολογιών καθώς και η έλλειψη κατάλληλης εκπαίδευσης πάνω στην εφαρμογή. Είναι γεγονός ότι οι παράγοντες επιτυχίας και αποτυχίας είναι σύνθετα ζητήματα και η διερεύνησή τους χρειάζεται

περεταίρω ανάλυση. (Κίτσιου, Σ., Βλαχοπούλου, Μ., 2008; Brender, J., Ammenwerth, E., Nykänen, P., Talmon, J. 2006).

1.8 Συμπεράσματα

Ιδιαίτερο ρόλο στον κλάδο της ιατρικής πληροφορικής αποτέλεσε τα τελευταία χρόνια το πληροφοριακό σύστημα υγείας. Σαν ΠΣΥ ορίζεται ένα ολοκληρωμένο σύστημα πληροφοριών ιατρικού ενδιαφέροντος το οποίο κατά βάση αποτελεί ένα σύνολο υλικού (hardware), λογισμικού (software) και ανθρώπινου δυναμικού (liveware) όπου στον πυρήνα του υπάρχει μία βάση δεδομένων με όλα τα απαραίτητα δεδομένα για την αποδοτική λειτουργία και διοίκηση μίας νοσοκομειακής μονάδας του οποίου οι χρήστες έχουν πρόσβαση στα συγκεκριμένα δεδομένα.

Η βασική διαφορά των συστημάτων αυτών από άλλα πληροφοριακά συστήματα είναι ότι χειρίζονται ανθρώπους, γεγονός που απαιτεί από το σύστημα να παρέχει αξιοπιστία, ασφάλεια και ευελιξία. Οι πληροφορίες που διαχειρίζεται ένα πληροφοριακό σύστημα υγείας είναι σε ψηφιακή μορφή και κατηγοριοποιούνται πολυεπίπεδα αναλόγως της θεματολογίας που άπτονται. Βέβαια, περαιτέρω εξειδικευμένες κατηγοριοποιήσεις γίνονται είτε βάσει χρονικής περιόδου συλλογής ή και ενδιαφέροντος είτε περιοχικά όσον αφορά τον τόπο συλλογής και χρησιμοποίησης. Ολοκληρωμένο χαρακτηρίζεται το σύστημα που εμπεριέχει πλήρες σύνολο κατηγοριών για όλων των ειδών τις πληροφορίες που το αφορούν. Έτσι, στην περίπτωση του ιατρικού συστήματος, πρέπει να υπάρχουν πληροφορίες τόσο διοικητικού-οικονομικού όσο και κλινικού, εργαστηριακού και φαρμακευτικού ενδιαφέροντος δομημένες με τέτοιον τρόπο ώστε να επιτρέπεται η γρήγορη, ασφαλής και ακριβής ενημέρωση ή συλλογή της πληροφορίας. Περνώντας, λοιπόν, σε διοικητικό επίπεδο (οικονομική διαχείριση, διαχείριση αρχείου ασθενών, διαχείριση υλικών αποθεμάτων κλπ.) μειώνεται ο χρόνος οργάνωσης και διεκπεραίωσης των διαφόρων εργασιών που θα ήταν χρονοβόρες χωρίς τη χρήση πληροφοριακών συστημάτων. Ακόμη, πρέπει να παρέχει τη δυνατότητα οριζόντιας διασύνδεσης με παρόμοια πληροφοριακά συστήματα που δε βρίσκονται στον ίδιο χώρο ώστε να συγκροτούν όλα αυτά μαζί ένα ευρύτερο σύστημα διαχείρισης πληροφοριών ιατρικού ενδιαφέροντος.

Οι μείζονος σημασίας παράγοντες που αφορούν σήμερα στην υλοποίηση ενός τέτοιου συστήματος εντοπίζονται στο χαρακτήρα που θα έχει η επικοινωνία και στις τεχνολογίες πληροφορικής που θα χρησιμοποιηθούν για το σκοπό αυτό. Όσον αφορά τον πρώτο παράγοντα, τίθεται θέματα ασφάλειας, διατήρησης του απορρήτου, χρηστικότητας και δυνατότητας εύκολης και εύλογης επεξεργασίας δεδομένων και εξαγωγής συμπερασμάτων. Επί της ουσίας, ίσως η μεγαλύτερη πρόκληση που αντιμετωπίζουν οι σχεδιαστές ιατρικών πληροφοριακών συστημάτων είναι η αυτοματοποίηση λειτουργιών που βασίζονται στην ανθρώπινη κρίση και εμπειρία με τρόπο τέτοιον ώστε η διακίνηση της ιατρικής πληροφορίας να

γίνεται με τρόπο αφενός ταχύ κι αφετέρου ικανό να διαφυλάξει την ανωνυμία των ασθενών. Για το δεύτερο παράγοντα, τίθεται θέματα συλλογής, αποθήκευσης και συμπίεσης δεδομένων, συμβατότητας και συνδεσιμότητας ηλεκτρονικών εργαλείων και τέλος, ταχύτητας και ασφάλειας μεταφοράς και μεταγωγής δεδομένων. Συγκεκριμένα, έχουν προταθεί κατά καιρούς διάφορες τυποποιημένες μορφές συλλογής στοιχείων που είναι ευρύτερες γνωστές, ανεξαρτήτως είδους, με την επωνυμία «Ιατρικός Φάκελος». Ο «Ιατρικός Φάκελος» δεν αναφέρεται απαραίτητα σε νοσηλευόμενο αλλά τόσο σε ιατρούς όσο και σε ερευνητές ή φοιτητές. Βέβαια, σε κάθε περίπτωση αυτός πρέπει να έχει διαφορετική μορφή αναλόγως το σκοπό και τις ανάγκες που εξυπηρετεί. Ο όγκος και η υφή των δεδομένων που θα έχει ο «Ιατρικός Φάκελος» έχουν ως συνέπεια την απαίτηση για δικτυακές συνδέσεις μεγάλου εύρους και αξιοπιστίας καθώς και υψηλών ταχυτήτων. Τα σύγχρονα μέσα μετάδοσης επιτρέπουν ένα τέτοιο είδος σύνδεσης αλλά προβλήματα μπορούν να εμφανιστούν λόγω πληθώρας πρωτοκόλλων μετάδοσης και της σχετικής ασυμβατότητας που τα διακρίνει. Γι' αυτό, άλλωστε, είναι καίρια η συμφωνία σ' ένα κοινό μοντέλο ανάπτυξης ιατρικού πληροφοριακού συστήματος.

Ωστόσο, το υλικό και το λογισμικό που απαιτούνται για την επίτευξη των υψηλών αυτών στόχων, κοστίζει πολλά χρήματα όπως άλλωστε και οι άνθρωποι που πρέπει να συνοδεύουν τον εξοπλισμό για να εκπαιδεύσουν και να βοηθήσουν τους μη καταρτισμένους εργαζόμενους. Αντιπαραβάλλοντας όμως δύο αντίθετους φαινομενικά παράγοντες (υψηλό κόστος-οφέλη), οι θετικές συνέπειες από τη εφαρμογή ενός τέτοιου συστήματος είναι διαχρονικές αλλά και μεγάλης σημασίας που όσο υψηλό κι αν είναι το κόστος ωχριά μπροστά τους.

Κεφάλαιο 2

Ζητήματα Διαλειτουργικότητας Πληροφοριακών Συστημάτων Υγείας

2.1 Εισαγωγή

Από τη φύση της η παροχή ιατρικής φροντίδας απαιτεί τη συνεργασία, επικοινωνία και την ανταλλαγή πληροφοριών μεταξύ των εμπλεκόμενων μερών. Σήμερα αυτό έχει καταστεί ευκολότερο λόγω της προόδου στην τεχνολογία. Έτσι μπορούν να διαβιβάζονται ηλεκτρονικά τα αρχεία υγείας μεταξύ των προμηθευτών, των γιατρών, των νοσοκομείων, των ασθενών και άλλων φορέων κατά την διάρκεια παροχής της ιατρικής φροντίδας (NCHICA, 2009).

Για την ανταλλαγή πληροφοριών υγείας το τελικό και σημαντικότερο στοιχείο είναι η σύνδεση μέσω του Διαδικτύου και άλλων δικτύων που επιτρέπει στους προμηθευτές υγειονομικής περίθαλψης να ανταλλάξουν τις πληροφορίες υγείας ασθενών. Η σύγχρονη όμως ιατρική υποδομή των πληροφοριακών συστημάτων αποτελείται από πολλά ετερογενή συστήματα με διαφορετικούς μηχανισμούς διαχείρισης δεδομένων. Επειδή όμως οι πληροφορίες των ασθενών χρειάζεται και πρέπει να είναι προσπελάσιμες από διαφορετικές θέσεις και συστήματα απαιτείται η ανάπτυξη προτύπων στοιχείων και μηνύματος για να καθιερώσουν τον κρίσιμο στόχο της διαλειτουργικότητας, δηλαδή τη δυνατότητα δύο ή περισσότερων συστημάτων π.χ. υπολογιστές, δίκτυα, πληροφοριακά συστήματα να επικοινωνήσουν το ένα με το άλλο και να κατανοήσουν τα στοιχεία που ανταλλάσσουν. Τα δίκτυα που επιτρέπουν την ηλεκτρονική επικοινωνία μεταξύ των προμηθευτών πρέπει να είναι ασφαλή προκειμένου να προστατευθούν οι πληροφορίες. Τέτοια πρότυπα επικοινωνίας είναι το HL7, το οποίο δημιουργήθηκε συγκεκριμένα για να παρέχει το κοινό πρωτόκολλο για τις διεπαφές ανταλλαγής για τα πληροφοριακά συστήματα. Ορίζει το περιεχόμενο, τη μορφή των δεδομένων με την οποία τα κλινικά και οικονομικά δεδομένα θα ανταλλάσσονται μεταξύ διαφορετικών υπολογιστικών συστημάτων υγείας. Επιπλέον καθορίζει τα trigger events και τα error messaging τα οποία προκύπτουν όταν η ανταλλαγή των δεδομένων δεν είναι επιτυχής. Το HL7 είναι ένα διεθνές σύνολο από ανοιχτά πρότυπα τα οποία επιτρέπουν την επικοινωνία αλλά και την ανεξάρτητη λειτουργία των διαφόρων συστημάτων πληροφοριών υγείας. (Orgun, B., 2003; Health Level Seven International, http://www.hl7.org/[22.9.2010])

Τα τελευταία χρόνια σε πολλές χώρες παγκοσμίως έχουν σημειωθεί σημαντικές προσπάθειες για την ενοποίηση μέσω τεχνολογιών «web services» πληροφοριακών συστημάτων, και την καθιέρωση ολοκληρωμένων πληροφοριακών υποδομών επικοινωνίας στην υγεία που θα

επιτρέψουν την απρόσκοπτη ανταλλαγή πολλαπλών, κατανεμημένων πληροφοριών και τη συντονισμένη επικοινωνία ανάμεσα σε οργανισμούς υγείας, τόσο σε περιφερειακό όσο και σε εθνικό επίπεδο (Κίτσιου, Σ., Βλαχοπούλου, Μ. 2008).

2.2 Διαλειτουργικότητα και Πληροφοριακά Συστήματα Υγείας

Υπάρχουν πολλοί ορισμοί για την διαλειτουργικότητα. Σύμφωνα με το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας, η διαλειτουργικότητα ορίζεται ως η δυνατότητα των Συστημάτων Πληροφορικής και Επικοινωνιών (Information and Communication Technology Systems) για ανταλλαγή δεδομένων και κοινή χρήση πληροφορίας και γνώσης. Σε αυτό το πλαίσιο διαλειτουργικότητας αναφέρεται και η διαλειτουργικότητα στο χώρο των υπηρεσιών υγείας που υποστηρίζουν τα ΠΣΥ.

Η παροχή υπηρεσιών υγείας από όλους όσους συμμετέχουν στα ΠΣΥ προϋποθέτει τη διακίνηση της πληροφορίας όπως αυτή αποκτάται και αποθηκεύεται πρωτογενώς. Συχνά η πληροφορία, ιδιαίτερα όταν αυτή αφορά τον ασθενή, πρέπει να διακινηθεί άμεσα και να έχει τους σωστούς αποδέκτες όπως για παράδειγμα στην περίπτωση διακομιδής του ασθενούς. Σε όλες τις περιπτώσεις δε θα πρέπει να υπάρχουν σημασιολογικές απώλειες σε πληροφοριακό επίπεδο. Η ανάγκη για διακίνηση της πληροφορίας διευκολύνεται και από τις νέες τάσεις για εφαρμογή των εργαλείων και υπηρεσιών eHealth που οδηγούν στο «κοινόχρηστο» ηλεκτρονικό φάκελο ασθενή (EHR κτλ) με σκοπό τη συνέχεια στη φροντίδα της υγείας του, τη διακίνηση ηλεκτρονικών παραπεμπτικών και άλλα.

Τα προβλήματα που πρέπει να αντιμετωπιστούν για την επίτευξη της κοινής χρήσης και διακίνησης της πληροφορίας στο Σύστημα Υγείας είναι:

- Το χαμηλό ποσοστό διαθεσιμότητας των Πληροφοριακών Συστημάτων στις διασυνδεδεμένες μονάδες υγείας, με αποτέλεσμα την δυσκολία στην ανταλλαγή δεδομένων,
- Τα ετερογενή συστήματα, που στηρίζουν τις μονάδες υγείας σε συνδυασμό με την έλλειψη προτυποποίησης των επικοινωνιακών υποδομών,
- Η ανάγκη αναδιοργάνωσης δομών και διαδικασιών, ώστε σε συνδυασμό με τις τεχνολογικές εξελίξεις να μπορούν να υποστηρίξουν την ανταλλαγή δεδομένων.

Γενικότερα, όταν τα ηλεκτρονικά δεδομένα μπορούν να οργανωθούν σε δομές και δομημένα μηνύματα ακολουθώντας δομημένη είσοδο δεδομένων και δομημένες κλινικές περιγραφές, η επικοινωνία γίνεται με πιο ασφαλή και ποιοτικό τρόπο χρησιμοποιώντας δομημένα μηνύματα και πληροφορία που ακολουθεί συγκεκριμένα πρότυπα, όσο αφορά την καταγραφή της και την σημασιολογία της.

2.2.1 Επίπεδα Διαλειτουργικότητας

Υπάρχουν διάφορα πλαίσια σύμφωνα με τα οποία ορίζονται οι κατηγορίες ή τα επίπεδα διαλειτουργικότητας. Τα επίπεδα διαλειτουργικότητας σύμφωνα με το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας είναι τα ακόλουθα:

Διαλειτουργικότητα σε επίπεδο επιχειρησιακό: Το επίπεδο αυτό στοχεύει στον καθορισμό των επιχειρησιακών στόχων και την συμμόρφωση των επιχειρησιακών διαδικασιών και της πληροφορίας των διαδικασιών αυτών, ώστε να επιτευχθεί η συνεργασία των υπηρεσιών και διοικήσεων που επιθυμούν να ανταλλάξουν πληροφορίες αλλά έχουν διαφορετικές δομές και διαδικασίες. Αφορά την διαλειτουργικότητα των διαδικασιών είτε εντός του οργανισμού είτε πολλών οργανισμών που συνεργάζονται.

Διαλειτουργικότητα σε επίπεδο σημασιολογικό: Αφορά την διασφάλιση ότι η πληροφορία που ανταλλάσσεται έχει την ίδια σημασία από κάθε αποδέκτη της. Για να επιτευχθεί η διαλειτουργικότητα στο επίπεδο αυτό είναι σημαντικά:

- Η ολοκλήρωση των δεδομένων (Data Integration)
- Η ολοκλήρωση σε λειτουργικό επίπεδο (Functional Integration) και
- Η ολοκλήρωση σε επίπεδο παρουσίασης (Presentation Integration)

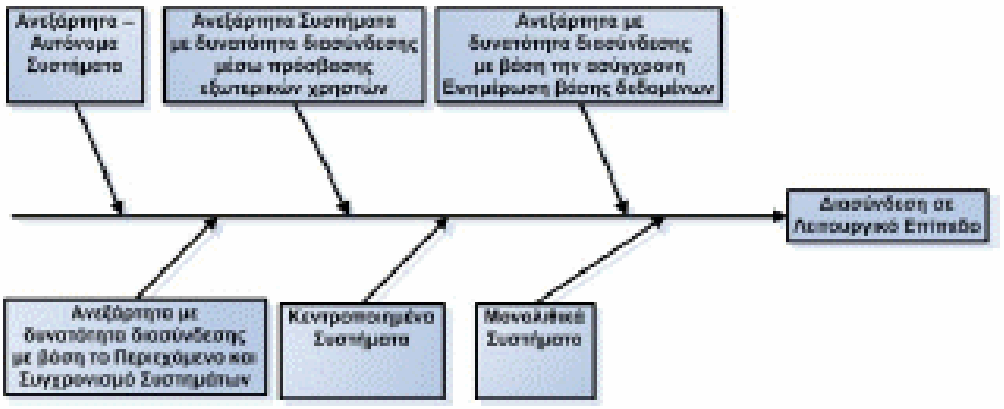
Διαλειτουργικότητα σε επίπεδο τεχνικό: Αφορά όλα τα τεχνικά θέματα για την ανταλλαγή της πληροφορίας και την διαλειτουργικότητα των υπολογιστικών συστημάτων και σχετικών υπηρεσιών.

Η διασύνδεση και η διαλειτουργικότητα των παρόχων υπηρεσιών υγείας, δηλαδή των νοσοκομείων και άλλων οργανισμών που συμμετέχουν στα δίκτυα υγείας, δεν είναι μόνο τεχνικό ζήτημα και ούτε αφορά μόνο την κοινή χρήση της πληροφορίας, αλλά επιτυγχάνεται και στα τρία διαφορετικά επίπεδα διαλειτουργικότητας. Και ενώ σήμερα υπάρχουν ευρέως γνωστά εργαλεία ολοκλήρωσης και διασύνδεσης σε τεχνικό επίπεδο (όπως message oriented middleware), η ανομοιογένεια των συστημάτων σε σημασιολογικό επίπεδο παραμένει σημαντικό εμπόδιο στη διαλειτουργικότητα των συστημάτων.

2.2.2 Διαλειτουργικότητα σε λειτουργικό επίπεδο

Σήμερα τα ΠΣΥ μπορούν να κατηγοριοποιηθούν σε έξι κατηγορίες ανάλογα με τη δυνατότητα διασύνδεσής τους σε λειτουργικό επίπεδο με σκοπό την ανταλλαγή δεδομένων υγείας αλλά και γενικότερα την ανταλλαγή δεδομένων που διακινούνται σε ένα δίκτυο υγείας (οικονομικά στοιχεία, στοιχεία προσωπικού, ιατρικός φάκελος ασθενή, επιδημιολογικά στοιχεία κτλ.). Η κατηγοριοποίηση στηρίχθηκε σε έρευνα που έχει γίνει σύμφωνα με τους Wilcox A et al. Έτσι τα συστήματα κατατάσσονται σε κατηγορίες ξεκινώντας από τα ανεξάρτητα συστήματα (separated

systems) με διάφορες διαβαθμίσεις, μέχρι και τα μονολιθικά (monolithic), όπως φαίνεται στο σχήμα 2.1



Σχήμα 2.1 *Κατηγοριοποίηση συστημάτων σύμφωνα με την δυνατότητα διασύνδεσης συστημάτων σε λειτουργικό επίπεδο*

Ανεξάρτητα Συστήματα: είναι αυτόνομα συστήματα τα οποία έχουν αναπτυχθεί εδώ και δεκαετίες πριν, όταν ο τρόπος επικοινωνίας ήταν μόνο το τηλέφωνο και το φαξ. Τα συστήματα αυτά -κυρίως εφαρμογές κλινικού φακέλου ασθενούς- είναι ευρέως χρησιμοποιούμενα από τους γιατρούς, χωρίς όμως να υπάρχει η δυνατότητα για την άντληση πληροφοριών-δεδομένων για τον ασθενή με άλλους τρόπους παρά μόνο με φαξ, τηλέφωνο ή επικοινωνία προσωπικά με τον γιατρό. Πρόκειται δε για σύγχρονη επικοινωνία. Σε έρευνα που έγινε από τον Overhage et al, γιατροί στα επείγοντα περιστατικά αντλούν πληροφορία για τον ασθενή από άλλον οργανισμό με φαξ ή τηλέφωνο για το 5% των ασθενών ξοδεύοντας 15,2 λεπτά ανά προσπάθεια επικοινωνίας. Έτσι, δεν υπάρχει συνέχεια στην παρακολούθηση του ασθενή-και γενικότερα στα δεδομένα του συστήματος υγείας- και ο μόνος τρόπος μεταφοράς πληροφορίας είναι ο ίδιος ο ασθενής- «οντότητα» που κουβαλά την ιατρική του «ταυτότητα».

Ανεξάρτητα Συστήματα με δυνατότητα πρόσβασης εξωτερικών χρηστών: είναι αυτόνομα εγκατεστημένα συστήματα στα νοσοκομεία/οργανισμούς αλλά επιτρέπουν την επικοινωνία σε εξωτερικούς χρήστες του συστήματος, κυρίως των γιατρών, για ανταλλαγή πληροφοριών (κυρίως σχετικά με τον ασθενή). Οι μέθοδοι που παρέχει ένα σύστημα για την πρόσβαση εξωτερικών χρηστών είναι διάφοροι και τα επίπεδα πρόσβασης ποικίλουν. Για παράδειγμα, είναι δυνατόν ένας γιατρός, αφού ταυτοποιηθεί ως αξιόπιστος χρήστης του συστήματος νοσοκομείου, να αποκτήσει πρόσβαση στον κλινικό φάκελο ασθενούς. Και ενώ τεχνικά είναι εφικτή η επικοινωνία των συστημάτων αυτών, ιδιαίτερα με την ανάπτυξη των εργαλείων του διαδικτύου, υπάρχουν νομικά ζητήματα σχετικά με την πρόσβαση εξωτερικών χρηστών σε προσωπικά δεδομένα και σε δεδομένα ασθενή. Η επικοινωνία στην περίπτωση αυτή είναι ασύγχρονη.

Ανεξάρτητα Συστήματα με δυνατότητα διασύνδεσης με ασύγχρονη ενημέρωση της βάσης δεδομένων: είναι τα αυτόνομα συστήματα σε οργανισμούς που μπορούν όμως και αντλούν στοιχεία-να επικοινωνούν-με άλλους οργανισμούς με ασύγχρονη επικοινωνία μέσω αιτημάτων και απαντήσεων για δεδομένα με χρήση μηνυμάτων. Πρόκειται για επικοινωνία σημείου προς σημείο (peer-to-peer) και προϋποθέτουν προτυποποίηση πληροφορίας ανάμεσα στα σημεία που επικοινωνούν. Για παράδειγμα, αν πρόκειται για ανταλλαγή πληροφορίας σχετική με τον ασθενή, απαιτείται κεντρικό Μητρώο Ασθενή στο οποίο θα έχουν πρόσβαση στα επικοινωνούντα μέρη για να αιτηθούν και να αντλήσουν την ταυτότητα του ασθενή τους ή να ενημερώσουν το ενιαίο κεντρικό Μητρώο. Επίσης, είναι απαραίτητο το κοινό μητρώο χρηστών ώστε να επιτρέπεται η πρόσβαση χρηστών στα ανεξάρτητα συστήματα. Η επικοινωνία γίνεται και σε αυτή την περίπτωση με ασύγχρονο τρόπο.

Ανεξάρτητα Συστήματα με δυνατότητα διασύνδεσης με βάση το περιεχόμενο και συγχρονισμό συστημάτων: είναι τα συστήματα στα οποία ο χρήστης έχει πρόσβαση ως πελάτης τους (client) και συγχρονίζονται όλα μαζί ανάλογα με την επιλογή του χρήστη σε ένα από αυτά. Έτσι, μπορεί σε ένα σταθμό εργασίας να είναι ανοιχτές πολλές εφαρμογές, και ο χρήστης, αποκτώντας πρόσβαση σε των εφαρμογών. Υλοποιήσεις τέτοιες έχουν γίνει με χρήση του προτύπου HL7 CCOW. Παρόλα αυτά είναι αναγκαίο τουλάχιστον το κοινό μητρώο ταυτοποίησης χρηστών και κοινό μητρώο δεδομένων (πχ ασθενή) βάσει των οποίων γίνεται ο συγχρονισμός με βάση το περιεχόμενο.

Κεντροποιημένα Συστήματα: αποτελούν επέκταση του προηγούμενου μοντέλου, όπου όλα τα δεδομένα συντηρούνται κεντρικά. Είναι τεχνικά εύκολη η υλοποίησή τους, στην πράξη, όμως, όλα τα δεδομένα που είναι για κοινή χρήση πρέπει να έχουν την ίδια δομή για τα συστήματα που διασυνδέονται καθώς και να υπάρχει κεντρική διαχείριση του συστήματος. Όλοι οι οργανισμοί στέλνουν τα δεδομένα τους δε μια κεντρική βάση με την ίδια δομή.

Μονολιθικά Συστήματα: είναι ιδιαίτερα δύσκολη η επικοινωνία και ουσιαστικά είναι επιτρεπτή μόνο ανάμεσα σε ίδια συστήματα ή με τις ίδιες παραμετροποιήσεις και μορφές στα δεδομένα. Η πρόσβαση στη συνέχεια είναι σχετικά απλή.

2.2.3 Προκλήσεις Διαλειτουργικότητας μεταξύ οργανισμών υγείας

Ο κύριος σκοπός της διαλειτουργικότητας μεταξύ των οργανισμών υγείας είναι η ανταλλαγή πληροφοριών μεταξύ τους. Αυτό απαιτεί την διασύνδεση και την ολοκλήρωση μεταξύ των οργανισμών. Κατά συνέπεια, για την επίτευξη της διαλειτουργικότητας θα πρέπει να εξεταστούν τα εξής ζητήματα:

- *Διασύνδεση (Interfacing):* ονομάζεται το όριο στο οποίο εμφανίζεται αλληλεπίδραση μεταξύ δύο συστημάτων ή διαδικασιών. Στην ορολογία πληροφορικής, υπάρχουν τρεις

τύποι διεπαφών: του χρήστη, του υλικού και του λογισμικού. Για παράδειγμα, η διεπαφή λογισμικού ορίζεται ως «οι γλώσσες και οι κώδικες που χρησιμοποιούνται από τις εφαρμογές για να επικοινωνούν μεταξύ τους».

- *Ολοκλήρωση (integration):* ονομάζεται ο συνδυασμός διαφορετικών εφαρμογών και η λειτουργία μιας κοινής συνεργασίας διαφόρων τμημάτων συστημάτων, με σκοπό τη διαμόρφωση μιας ενιαίας οντότητας. Η ολοκλήρωση πρέπει να περιλαμβάνει μια προδιαγραφή κατάλληλων προτύπων και μια πλατφόρμα επικοινωνίας που ενδεχομένως καθιστά δυνατή τη διαλειτουργικότητα μεταξύ των οργανισμών, διαφορετικά η ολοκλήρωση δεν θα πραγματοποιούνταν.
- *Δυνατότητα Πρόσβασης (Accessibility):* είναι πολύ σημαντικό να εστιάσουμε στη δυνατότητα πρόσβασης όταν επικοινωνούν διαφορετικοί οργανισμοί υγειονομικής περίθαλψης. Το ερώτημα που γεννάται είναι το ποιος έχει πρόσβαση σε κοινές ιατρικές πληροφορίες και σε ποιο επίπεδο, μέσω του συστήματος. Έτσι, είναι καλύτερη η παροχή ενός τρόπου πρόσβασης των κλινικών πληροφοριών μέσω του συστήματος.
- *Ιδιωτικότητα (Privacy):* Η δυνατότητα πρόσβασης ακολουθείται από την ιδιωτικότητα. Μόλις υπάρξει πρόσβαση στις πληροφορίες, αμέσως εγείρεται το πρόβλημα της ιδιωτικότητας. Προκειμένου να αντιμετωπιστεί το πρόβλημα της ιδιωτικότητας, θα πρέπει να υπάρξει πρόσβαση στις πληροφορίες μόνο από εξουσιοδοτημένους χρήστες που έχουν την άδεια να χρησιμοποιήσουν το σύστημα.
- *Ασφάλεια (Security):* Προκειμένου να διανεμηθούν οι ιατρικές πληροφορίες στον ίδιο τον ασθενή αλλά και σε άλλους οργανισμούς υγειονομικής περίθαλψης, σύμφωνα με το νόμο (HIPAA), υπάρχει η ανάγκη ώστε η κατάλληλη εξουσιοδότηση και συγκατάθεση να αλληλεπιδράσουν με τις ιατρικές πληροφορίες. Πιο συγκεκριμένα νοείται, το ποιος μπορεί να έχει πρόσβαση στα δεδομένα ασθενών, σε ποιο επίπεδο και πότε. Αυτό αναμφιβόλως, επιβαρύνει τη διαδικασία διανομής των ιατρικών πληροφοριών των ασθενών. Εξαιτίας αυτού, οι οργανισμοί υγειονομικής περίθαλψης πρέπει να παρέχουν το κατάλληλο επίπεδο ασφάλειας και επίσης να επιβεβαιώνουν ότι τα συστήματά τους την παρέχουν.

2.3 Πρότυπα και Κωδικοποιήσεις

Κάθε ΠΣΥ που στοχεύει στην πλήρη ικανοποίηση των αναγκών των ιατρών, αλλά και όλων των υπολοίπων που εμπλέκονται στη διαχείριση ασθενών και πόρων ενός νοσοκομείου, είναι απαραίτητο να υποστηρίζει ένα σύνολο κωδικών και προτύπων, που θα καθορίζουν τον τρόπο συλλογής, συνεργασίας και παρουσίασης των δεδομένων από διαφορετικά πληροφοριακά συστήματα. Η ανταλλαγή των πληροφοριών μεταξύ πληροφορικών συστημάτων τα οποία έχουν

σχεδιαστεί και κατασκευαστεί με διαφορετικούς κανόνες και μεθοδολογίες, απαιτεί την ύπαρξη ενός δικτύου το οποίο με χρήση hardware και πολλών ίσως επιπέδων και λειτουργικών μονάδων λογισμικού, καταφέρνει να συνδέσει όλα αυτά τα συστήματα. «Πρωτόκολλα Επικοινωνίας» ονομάζουμε καλά ορισμένες μεθόδους και κανόνες που ακολουθούνται ώστε να εξασφαλίζεται η ορθή επικοινωνία μεταξύ διαφορετικών πληροφοριακών συστημάτων.

Ένα σύνολο πρωτοκόλλων και τα επίπεδα στα οποία αυτά χρησιμοποιούνται, αποτελούν τα «Πρότυπα Επικοινωνίας» (communication standards). Αυτά τα πρότυπα αναφέρονται στον τρόπο με τον οποίο πρέπει να γίνονται οι μεταφορές πληροφορίας από ένα σύστημα σε κάποιο άλλο καθώς και σε αυτή καθ' αυτή την πληροφορία που μπορεί να μεταφέρεται. Τα πρότυπα που αφορούν στα πληροφοριακά συστήματα στο χώρο της υγείας μπορούν να χωριστούν στις παρακάτω κατηγορίες:

- Πρότυπα επικοινωνίας
- Πρότυπα για την αναπαράσταση των κλινικών δεδομένων (κωδικοποιήσεις)
- Πρότυπα αναγνώρισης
- Πρότυπα ασφάλειας των δεδομένων και εξασφάλισης ιατρικού απόρρητου.

Με χρήση προτύπων για κάθε μια από τις παραπάνω κατηγορίες καθώς και με υιοθέτηση πρωτοκόλλων επικοινωνίας μπορεί να επιτευχθεί «διαλειτουργικότητα» μεταξύ των συστημάτων. Στη συνέχεια, ακολουθεί μια σύντομη αναφορά των βασικότερων προτύπων κάθε είδους, όπως αυτά έχουν διαμορφωθεί ως σήμερα.

2.3.1 Πρότυπα επικοινωνίας

CEN/TC 251: Η Ευρωπαϊκή Επιτροπή Τυποποίησης (European Standards Committee-CEN) έχει δημοσιεύσει ένα pre-standard για την αρχιτεκτονική Ηλεκτρονικού Ιατρικού Φακέλου (Electronic HealthCare Record) με την ονομασία ENV 13606. Αυτό ορίζει γενικές δομές πληροφορίας και χαρακτηριστικά κοινά σε κάθε ηλεκτρονικό ιατρικό φάκελο, δηλαδή ένα λογικό μοντέλο, χωρίς να καθορίζει ακριβώς τι ιατρική πληροφορία θα περιέχει ή πώς θα υλοποιηθεί. Το ENV 13606 είναι το μόνο πρότυπο ειδικά για ηλεκτρονικό ιατρικό φάκελο στον κόσμο και δεν έχει υλοποιηθεί σε κάποιο σύστημα, αποτελεί όμως αναφορά και υπάρχουν προσπάθειες συνεργασίας και εναρμονισμού της CEN/TC 251 και άλλων προτύπων, όπως το HL7.

Σκοπός του CEN είναι να παράγει μια ακριβή, άκαμπτη και μεγάλη σε διάρκεια αρχιτεκτονική η οποία να παριστάνει τον Ηλεκτρονικό Ιατρικό Φάκελο. Στόχος είναι να υποστηρίζει την διαλειτουργικότητα των συστημάτων καθώς και τις συνιστώσες οι οποίες χρειάζονται για να αλληλεπιδρούν οι υπηρεσίες του Ηλεκτρονικού Ιατρικού Φακέλου ως:

- Διακριτά συστήματα

- Να έχει πρόσβαση, να μεταφέρει, να προσθέτει καθώς και να μορφοποιεί διάφορες εισόδους νέων ιατρικών φακέλων
- Να κάνει χρήση ηλεκτρονικών μηνυμάτων ή κατανεμημένων αντικειμένων
- Να διατηρεί το αρχικό κλινικό δεδομένο που προηγείται από τον σχεδιαστή του.

ISO/TC 215: Ο οργανισμός τυποποίησης ISO έχει ιδρύσει την Τεχνική Επιτροπή 215 (TC 215) με στόχο την προτυποποίηση στον τομέα της ιατρικής πληροφορικής (Health Informatics). Τα πρότυπα (standards) κατά ISO/TC 215 είναι η παγκόσμια κορυφή για τον ΗΙΦ, όπως και για άλλα πρότυπα που αφορούν στην Ιατρική Πληροφορική.

Κάποιοι οργανισμοί έκαναν χρήση ήδη συγκεκριμένων προτυποποιήσεων διεθνών οργανισμών, όπως είναι το ISO. Μερικοί από τους οργανισμούς που το έκαναν αυτό είναι οι DICOM, IEEE, CEN, HL7. Είναι γνωστό άλλωστε πως οι τρείς τελευταίοι οργανισμοί έχουν ειδική συμφωνία με τον ISO που εξουσιοδοτούν τις υπάρχουσες προτυποποιήσεις προκειμένου να γίνουν πρότυπα κατά ISO.

Ο οργανισμός ISO/TC 215 έχει έξι ομάδες εργασίας (working groups) οι οποίες είναι οι παρακάτω:

- WG1: Ιατρικοί φάκελοι και συντονισμός των μοντέλων. Η επιδίωξη είναι ένα πρότυπο ιατρικού φακέλου, όπου η κατάλληλη πληροφορία θα είναι διαθέσιμη όταν και όπου απαιτείται η υποστήριξη αποφάσεων.
- WG2: Μετάδοση πληροφορίας και επικοινωνία
- WG3: Αναπαράσταση ιατρικών ήχων
- WG4: Ασφάλεια
- WG5: Ιατρικές κάρτες
- WG6: Ηλεκτρονικό φαρμακείο

HL7: Ο οργανισμός Health Level Seven Inc. (HL7) σχηματίστηκε το 1987 στις Η.Π.Α. με σκοπό την ανάπτυξη προτύπων σχετικά με την ηλεκτρονική ανταλλαγή δεδομένων και την αυτόματη ανταλλαγή πληροφορίας μεταξύ των διαφορετικών πληροφοριακών συστημάτων στην υγειονομική περίθαλψη.

Το HL7 είναι το πλέον ευρέως χρησιμοποιημένο πρότυπο ανταλλαγής πληροφοριών μέσω μηνυμάτων σε κλινικό περιβάλλον. Χρησιμοποιείται σε όλες τις ηπείρους. Εάν περιοριστεί κανείς στην Ευρώπη θα δει ότι χρησιμοποιείται σχεδόν σε κάθε χώρα ως πρότυπο ανταλλαγής πληροφοριών μέσω μηνυμάτων ανάμεσα στα διάφορα υποσυστήματα. Σχεδόν όλα τα ευφυή διαγνωστικά μηχανήματα (ιατροτεχνολογικός εξοπλισμός) μπορούν να "μιλήσουν" HL7 και σχεδόν όλα τα ιατρικά πληροφοριακά συστήματα υψηλού επιπέδου είναι σε θέση να στείλουν

και να λάβουν τα κατάλληλα HL7 μηνύματα, χρησιμοποιώντας τους κανόνες ανταλλαγής μηνυμάτων του HL7 (του πρωτοκόλλου).

Επίσης το HL7 είναι ξεκάθαρα το πιο ώριμο πρότυπο ανταλλαγής πληροφοριών μέσω μηνυμάτων. Η έρευνα από την ακαδημαϊκή κοινότητα και την βιομηχανία και τις εταιρίες συμβούλων οδήγησε σ' αυτό το πρότυπο, την κυριότητα του οποίου την κατέχει ο μη κερδοσκοπικός οργανισμός Health Level Seven Inc. Ο οποίος έχει τοπικά υποκαταστήματα σε όλες σχεδόν τις χώρες της Ευρώπης, στις Ηνωμένες Πολιτείες της Αμερικής, στην Αυστραλία / Νέα Ζηλανδία, την Ασία και στη ζώνη του Ειρηνικού.

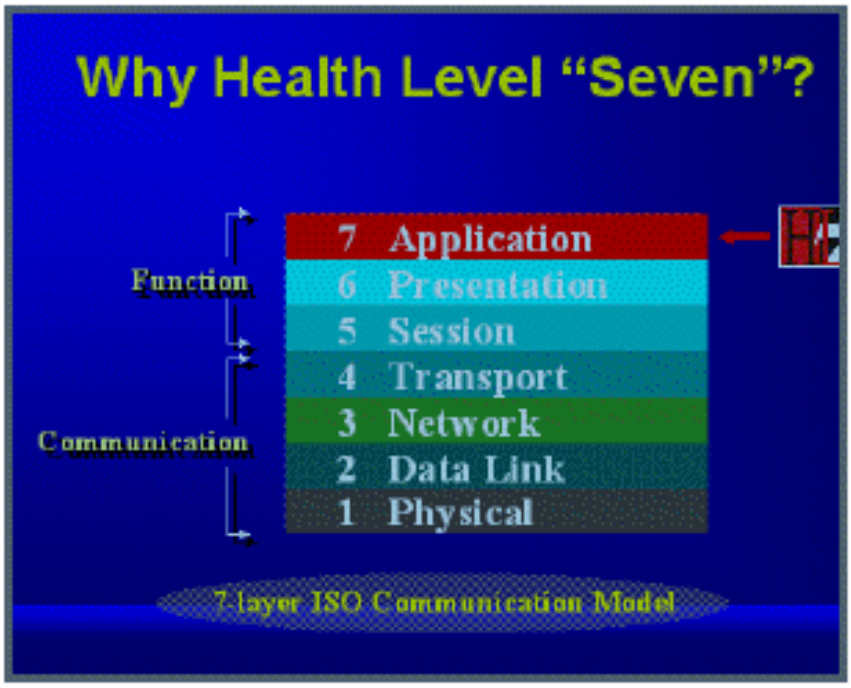
Το πρότυπο HL7 έχει αναγνωριστεί από πολλά εθνικά ιδρύματα προτυποποίησης, όπως ο ANSI (USA) και ο DIN (Γερμανία). Επίσης, το HL7 χρησιμοποιείται καθημερινά σε εκατοντάδες νοσοκομεία σε όλο τον κόσμο, συνδέοντας μια μεγάλη ποικιλία εφαρμογών και συστημάτων.

Η αποστολή του οργανισμού "HL7 Inc." είναι η δημιουργία αξιόπιστων προτύπων ανταλλαγής, διαχείρισης και ολοκλήρωσης δεδομένων που αφορούν την κλινική φροντίδα του ασθενή, και την διαχείριση, οργάνωση και αξιολόγηση υπηρεσιών ιατρικής περίθαλψης. Ο οργανισμός ενθαρρύνει τη δημιουργία ευέλικτων προτύπων, οδηγιών, μεθοδολογιών, πρωτοκόλλων και άλλων συναφών υπηρεσιών και προϊόντων, προκειμένου να καταστεί εφικτή η διαλειτουργικότητα πληροφοριακών συστημάτων στην Υγεία - Πρόνοια και η ανταλλαγή στοιχείων του ηλεκτρονικού φακέλου ασθενή.

Ο οργανισμός "HL7 Inc." δημιουργήθηκε προκειμένου να λειτουργεί ως αξιόπιστο μέσο επικοινωνίας μεταξύ των ενδιαφερομένων φορέων στον τομέα της ιατρικής περίθαλψης, γεγονός που αποτυπώνεται στην ποικιλία που παρουσιάζουν τα μέλη του όπως εταιρίες ιατρικής πληροφορικής, ιδιωτικοί και δημόσιοι φορείς υγείας - πρόνοιας, ειδικοί σύμβουλοι, εμπειρογνώμονες, εταιρίες ολοκλήρωσης πληροφοριακών συστημάτων (system integrators),ασφαλιστικοί φορείς, εταιρίες ιατροτεχνολογικού εξοπλισμού, φορείς παροχής υπηρεσιών υγείας - πρόνοιας, κλπ.

Αναγνωρίζοντας λοιπόν την ανάγκη υποστήριξης των τοπικών ομάδων που δραστηριοποιούνται στην προώθηση των προτύπων, ο "HL7 Inc." στηρίζει τις προσπάθειες αυτές με την δημιουργία τοπικών παρατημάτων (HL7 affiliates). Μέχρι σήμερα έχουν ήδη ιδρυθεί 23 τέτοια παραρτήματα (Ηνωμένο Βασίλειο, Καναδάς, Αυστραλία, Νέα Ζηλανδία, Νότιος Αφρική, Γερμανία, Ολλανδία, Φιλανδία, Ινδία, Ιαπωνία, Αργεντινή, Κίνα, Κορέα, Τσεχία, Λιθουανία, Ελβετία, Βραζιλία, Κροατία, Μεξικό, Ιταλία, _ανία και Ταϊβάν). Τα τοπικά παραρτήματα είναι ανεξάρτητοι οργανισμοί διεθνούς χαρακτήρα που στοχεύουν στην ανάπτυξη, υποστήριξη, αποδοχή και χρήση των προτύπων HL7 σε παγκόσμια κλίμακα με την μεταφορά αυτών στην αντίστοιχη γλώσσα του παραρτήματος.

Το HL7 προτυποποιεί τα πρωτόκολλα και τις δομές για την ανταλλαγή μηνυμάτων ιατρικού ενδιαφέροντος στο επίπεδο της εφαρμογής, στο 7 επίπεδο του μοντέλου OSI, δηλαδή είναι ανεξάρτητο από συγκεκριμένες πλατφόρμες και τεχνολογίες.



Σχήμα 2.2 *Πρότυπο HL7*

Οι εκδόσεις HL7 2.x παρά την ευρύτερη αποδοχή και τις υλοποιήσεις, παρουσιάζουν αρκετά μειονεκτήματα, και συγκεκριμένα:

- Δεν υπάρχει ένα λογικό μοντέλο αναφοράς της πληροφορίας που ανταλλάσσεται στα μηνύματα, ούτε τρόπος αναπαράστασης της σχέσης μεταξύ των δεδομένων.
- Χρησιμοποιεί πολύ ειδική σύνταξη στα μηνύματα, καθιστώντας δύσκολη την εκμάθηση και την υλοποίηση του προτύπου.
- Έχει πολλά προαιρετικά χαρακτηριστικά, κάτι που παρέχει ευελιξία και συνεισφέρει αποφασιστικά στη διάδοσή του, αλλά και που καθιστά σχεδόν αδύνατο τον έλεγχο της συμμόρφωσης προς το πρότυπο των διαφόρων υλοποιήσεων. Έτσι απαιτείται μεγάλη προσπάθεια για να εξασφαλισθεί ότι οι δύο εφαρμογές που θα «μιλήσουν μεταξύ τους, χρησιμοποιούν τα ίδια χαρακτηριστικά».

Η έκδοση HL7 Version 3, αντιμετωπίζει ουσιαστικά τα παραπάνω θέματα.

2.3.2 Πρότυπα κλινικών δεδομένων

Για την παρουσίαση των κλινικών δεδομένων έχουν δημιουργηθεί πολλά πρότυπα ειδικά για να εκφράσουν με συστηματικό τρόπο διαγνώσεις και διαδικασίες. Σήμερα υπάρχουν πάνω από 150 γνωστά συστήματα κωδικοποίησης αλλά αυτά με την ευρύτερη αποδοχή είναι:

Διεθνής Κατηγοριοποίηση Ασθενειών - International Classification of Diseases (ICD): Η ICD κωδικοποίηση είναι ήδη στην 9η έκδοση (ICD-9): Αυτοί οι κωδικοί συντηρούνται από την Παγκόσμια Οργάνωση Υγείας (WHO) και είναι αποδεκτοί παγκοσμίως. Στις Η.Π.Α. το Εθνικό Κέντρο Στατιστικής για την Υγεία (National Centre for Health Statistics-NCHS) και το Κέντρο Οικονομικής Διαχείρισης των Οργανισμών Υγείας (Health Care Financing Administration-HCFA) στις ΗΠΑ έχουν υποστηρίξει την ανάπτυξη κάποιων αλλαγών για τους κωδικούς του ICD-9 και έχουν έτσι δημιουργήσει το ICD-9-CM (http://www.cs.umu.se/~medinfo/ICD9.html). Η WHO έχει αναπτύξει το ICD-10 και το HCFA έχει δημιουργήσει μια εθελοντική ομάδα για να βοηθήσει στην ανάπτυξη του συστήματος κωδικοποίησης διαδικασιών (Procedure Coding System ICD-10-PCS). Παρόλα αυτά το HCFA προβλέπει πως το ICD-10 δεν θα είναι διαθέσιμο για χρήση στις ΗΠΑ για μερικά χρόνια ακόμα. Γεγονός είναι πως στις ΗΠΑ οι ασφαλιστικές εταιρείες, απαιτούν τη χρήση του ICD-9-CM για να δώσουν τις όποιες αποζημιώσεις, αλλά σε ότι αφορά την αξία των κωδικών αυτών σε ότι έχει να κάνει με το κλινικό μέρος, αυτή θεωρείται πολύ περιορισμένη λόγω της έλλειψης κλινικής σαφήνειας. Επιπλέον η διαδικασία επιλογής και εισαγωγής του κωδικού της κατάλληλης ασθένειας είναι αρκετά δύσκολο να γίνει από άτομα που δεν έχουν ιατρικές γνώσεις (http://www3.who.int/icd/vol1htm2003/fr-icd.htm).

Read Codes: Οι Read Codes αναπτύχθηκαν στη Μεγάλη Βρετανία και είναι ουσιαστικά μια εκτενής λίστα όρων που χρησιμοποιούνται στο χώρο της υγείας. Ο στόχος είναι να χρησιμοποιηθεί από όλους όσους ασχολούνται με την υγεία και θέλουν να περιγράψουν την θεραπευτική αγωγή και την περίθαλψη των ασθενών τους. Έχει γίνει ιδιαίτερη προσπάθεια ώστε με τη χρήση των Read Codes να μπορεί κανείς να περιγράψει όσο το δυνατόν περισσότερων ειδών πληροφορία έχει να κάνει με την κατάσταση κάποιου ασθενή, σχεδόν σε φυσική γλώσσα, αλλά με κωδικοποιημένο τρόπο ώστε να μπορεί να καταχωρηθεί και να αναζητηθεί από ένα σύστημα πληροφορικής. Καλύπτουν λοιπόν θέματα όπως επαγγέλματα, σημάδια και συμπτώματα, εξετάσεις, διαγνώσεις, θεραπευτικές αγωγές και θεραπείες, φάρμακα και με τις εφαρμογές τους και αρκετές ακόμα περιπτώσεις. Αυτό μπορεί να κάνει δυνατή την αποθήκευση σε έναν υπολογιστή σχεδόν οποιουδήποτε σχετικού με την υγεία κειμένου, από την συνοπτική περιγραφή κάποιου επεισοδίου μέχρι έναν πλήρη ηλεκτρονικό φάκελο ασθενή, εάν αυτό είναι επιθυμητό.

Ο κάθε όρος έχει ένα μοναδικό κωδικό ο οποίος βρίσκεται αποθηκευμένος στον υπολογιστή. Έτσι επιτρέπεται η αποθήκευση, η αναζήτηση και η ανάλυση των δεδομένων. Όταν η πληροφορία επιστρέφεται στην οθόνη, ο γιατρός βλέπει μπροστά του, όχι τον κωδικό αλλά τον οικείο ιατρικό όρο που περιγράφει την κατάσταση. Οι Read Codes θα μπορούσαν ίσως να

κάνουν τον Ιατρικό Φάκελο εύκολα επανακτήσιμο. Είναι γεγονός ότι οι κωδικοί μπορούν να κάνουν τα αρχεία των ασθενών εύκολα αναζητήσιμα και ανακτήσιμα. Η δομημένη μορφή του ιατρικού φακέλου στον υπολογιστή μπορεί να προσπελαστεί και να χρησιμοποιηθεί για να λύσει πολλά προβλήματα που έχουν να κάνουν με την περίθαλψη του ασθενή. Οι Read Codes έχουν εγκριθεί από το συνέδριο του Royal Medical Colleges. ΤΟ 1998 το Joint Computer Group του RCGP και η General Medical Services Committee του BMA πρότεινε να χρησιμοποιηθούν οι Read Codes σαν το πρότυπο στα πληροφορικά συστήματα των κλινικών.

Οι πρόσφατες έρευνες στην Μεγάλη Βρετανία δείχνουν ότι το 87% των γραφείων των οικογενειακών γιατρών είναι μηχανογραφημένα. Από αυτά, περισσότερα από 60% χρησιμοποιούν Read Codes και είναι πάρα πολύ πιθανό αυτό το ποσοστό να φτάσει το 90% τα επόμενα 2-3 χρόνια. Το κέντρο για την κωδικοποίηση και την κατηγοριοποίηση (Centre for Coding and Classification NHS) του Εθνικού Συστήματος Υγείας της Μεγάλης Βρετανίας, έχει αναλάβει να αναπτύξει τους Read Codes ώστε να χρησιμοποιηθούν από όλους τους επαγγελματίες στο χώρο της υγείας. Η ανάπτυξη καθοδηγείται από μέλη του Royal Colleges and Associations, συμπεριλαμβανομένων και νοσοκόμων και άλλων επαγγελμάτων που έχουν να κάνουν με το χώρο της υγείας.

Systematized Nomenclature of Human & Veterinary Medicine (SNOMED): Η διεθνής κωδικοποίηση με την ονομασία Systematized Nomenclature of Human and Veterinary Medicine (SNOMED), συντηρείται από το College of American Pathologists (CAP) και είναι ευρέως αποδεκτή για την περιγραφή αποτελεσμάτων παθολογοανατομικών (ιστολογικών) εξετάσεων. Έχει πολύ-αξονική δομή κωδικοποίησης (έντεκα πεδία) η οποία επιτρέπει μεγαλύτερη σαφήνεια σε σχέση με την κωδικοποίηση ICD και έχει σημαντική αξία όσον αφορά το κλινικό κομμάτι. Το CAP έχει αρχίσει να εναρμονίζει το SNOMED με τα πρότυπα HL7 και ACR-NEMA. Το SNOMED αποτελεί ένα από τους πρώτους υποψήφιους για να γίνει το πρότυπο για τον ιατρικό φάκελο βασισμένο σε υπολογιστή.

Diagnosis Related Group (DRG): Ένα DRG είναι η κατηγοριοποίηση μιας επίσκεψης σε κάποιο νοσοκομείο από την άποψη του ποιο ήταν το πρόβλημα και πως αντιμετωπίστηκε σε κάποιον ασθενή. Η κατηγοριοποίηση DRG (μια από τις περίπου 500) προσδιορίζεται από ένα πρόγραμμα ομαδοποίησης (grouper) το οποίο βασίζεται σε διαγνώσεις και διαδικασίες κωδικοποιημένες με το ICD-9-CM καθώς και σε στοιχεία του ασθενή όπως ηλικία, φύλο, διάρκεια παραμονής στο νοσοκομείο και άλλους παράγοντες. Συνήθως το DRG προσδιορίζει το ποσό που θα κοστίσει μια επίσκεψη (με την ευρεία έννοια) ανεξάρτητα από τις χρεώσεις που έχουν προκύψει. Οι κωδικοί DRG έχουν αξία κυρίως για να διευκολύνουν τέτοιου είδους οικονομικές αναλύσεις και όχι για κλινικές έρευνες ή θεραπευτική αγωγή στους ασθενείς, καθώς δεν έχουν την απαραίτητη κλινική σαφήνεια.

2.3.3 Πρότυπα αναγνώρισης

Αυτά τα πρότυπα καλύπτουν την ανάγκη για ύπαρξη κάποιων μοναδικών κωδικών (αναγνωριστικά-προσδιοριστές) που να προσδιορίζουν με μοναδικό τρόπο κάθε ασθενή, πάροχο υπηρεσίας, οργανισμό ή προϊόν. Πρέπει παρόλα αυτά να σημειωθεί πως δεν υπάρχει μέχρι σήμερα κάποια καθολική αποδοχή και ικανοποίηση από αυτά τα συστήματα.

Αναγνωριστικά Ασθενών: Ο αριθμός κοινωνικής ασφάλισης (Social Security Number-SSN) θεωρείται σαν ένας αριθμός ο οποίος προσδιορίζει μοναδικά κάθε ασθενή στις ΗΠΑ. Εντούτοις, οι κριτικές επιμένουν ότι δεν μπορεί να θεωρηθεί σαν τέτοιος απλά και μόνο γιατί ο καθένας δεν έχει έναν SSN η ακόμα χειρότερα μπορεί να χρησιμοποιούν τον ίδιο αριθμό SSN διάφοροι πολίτες ή τέλος λόγω της ευρείας χρήσης που έχει αυτός ο αριθμός υπάρχουν μεγάλοι κίνδυνοι σε ότι έχει να κάνει με το ιατρικό απόρρητο και την ασφάλεια. Αυτά τα ζητήματα έχουν ήδη τονιστεί από την επιτροπή E31.12 του ASTM (American Society for Testing and Materials) η οποία δημιούργησε το «Guide for the properties of a Universal Healthcare Identifier (UHID)». Το ινστιτούτο CPRI (Computer-Based Patient Record Institute) έχει μια ομάδα η οποία έχει επίσης ερευνήσει αυτά τα ζητήματα και ετοιμάζει μια εκτεταμένη και περιεκτική δημοσίευση.

Αναγνωριστικά Παρόχων: Το Κέντρο Οικονομικής Διαχείρισης των Οργανισμών Υγείας (Health Care Financing Administration-HCFA) στις ΗΠΑ έχει δημιουργήσει έναν ευρέως χρησιμοποιούμενο προσδιοριστή, γνωστό με το όνομα «Universal Physician Identifier Number-UPIN». Ο UPIN δίνεται μόνο σε γιατρούς οι οποίοι δουλεύουν με ηλικιωμένους ασθενείς. Για να ξεπεράσει αυτόν τον περιορισμό, το HCFA αναπτύσσει το Εθνικό Αρχείο Παρόχων «National Provider File-NPF».

Αναγνωριστικά Τόπου Περίθαλψης: Υπάρχουν δύο ευρέως χρησιμοποιούμενα αναγνωριστικά-προσδιοριστές τόπων περίθαλψης. Το ένα είναι το «Health Industry Number-HIN», το οποίο προέκυψε από το «Health Industry Business Communications Council-HIBCC». Το HIN είναι ένα αναγνωριστικό για οικογενειακούς γιατρούς και φαρμακεία λιανικής. Το HCFA έχει επίσης ορίσει έναν πάροχο αναγνωριστικών για χρήση από όσους ασχολούνται με ηλικιωμένους ασθενείς (Medicare).

Προσδιοριστές Προϊόντων και Ετικετών Προμηθειών: Σε αυτή την περιοχή χρησιμοποιούνται κυρίως τρεις προσδιοριστές.

- Ο «Labeller Identification Code-LIC» ο οποίος χρησιμοποιείται για να προσδιορίσει τον κατασκευαστή ή τον διανομέα και παρέχεται από το HIBCC.
- Ο LIC χρησιμοποιείται με ή χωρίς bar codes για προϊόντα και προμήθειες που διανέμονται μέσα σε κάποιο οργανισμό παροχής υπηρεσιών υγείας.
- Ο κωδικός «Universal Product Code-UPC» συντηρείται από το Uniform Code Council και χρησιμοποιείται για ετικέτες προϊόντων τα οποία πωλούνται σε τιμές λιανικής.

2.3.4 Πρότυπα Εξασφάλισης του απορρήτου των δεδομένων

Οι βασικότεροι κίνδυνοι κατά τη μετάδοση ενός ηλεκτρονικού μηνύματος είναι:

- Υποκλοπή της πληροφορίας
- Αλλοίωση της πληροφορίας
- Παραποίηση της ταυτότητας του παραλήπτη ή/και του αποστολέα

Στις μέρες μας αντιμετωπίζονται μεγάλες αδυναμίες στα θέματα ασφάλειας και συνεχώς νέα θεσμικά θέματα και πιέσεις στην αγορά οδηγούν στον επανασχεδιασμό των ιατρικών πληροφοριακών συστημάτων, δίνοντας έμφαση στην ασφάλεια. Οι κυριότερες πτυχές της ασφάλειας αναφέρονται παρακάτω:

- *Πιστοποίηση:* Έλεγχος της αυθεντικότητας της ταυτότητας των μερών μιας ανταλλαγής δεδομένων
- *Εξουσιοδότηση:* Η πρόσβαση του χρήστη πρέπει να είναι εξουσιοδοτημένη και να βασίζεται στο δικαίωμα πρόσβασης του χρήστη. Η πρόσβαση πρέπει να απαγορεύεται σε μη εξουσιοδοτημένα άτομα.
- *Εμπιστευτικότητα:* Η τήρηση του απορρήτου των δεδομένων – η πληροφορία διατίθεται μόνο σε εκείνους τους χρήστες που είναι εξουσιοδοτημένοι.
- *Ακεραιότητα:* Τα δεδομένα θα πρέπει να παραμένουν ακέραια, δηλαδή να μην υποστούν αλλοίωση.
- *Αδυναμία άρνησης συμμετοχής:* Ο χρήστης δεν μπορεί να αρνηθεί την συμμετοχή του στην ανταλλαγή δεδομένων.
- *Δυνατότητα ελέγχου:* Κάθε τροποποίηση ή επεξεργασία των δεδομένων πρέπει να μπορεί να ελεγχθεί, δηλαδή από ποιον έγινε και πότε.
- *Ευθύνη:* Καθορισμός της ευθύνης για την εισαγωγή, πρόσβαση ή τροποποίηση κάθε δεδομένου.
- *Διαφάνεια:* Τεκμηρίωση των διαδικασιών της επεξεργασίας ώστε να μπορούν να ελεγχθούν.
- *Διαθεσιμότητα:* Τα δεδομένα και οι υπηρεσίες πρέπει να είναι διαθέσιμα όταν χρειάζεται.

Η ανάπτυξη συστημάτων ιατρικού φακέλου βασισμένων σε υπολογιστή καθώς και δικτύων υπολογιστών ανάμεσα σε οργανισμούς υγείας, δημιούργησαν την ανάγκη για ανάπτυξη προτύπων και μεθόδων που θα εξασφαλίσουν το ιατρικό απόρρητο και την ασφάλεια των δεδομένων. Οι παρακάτω δραστηριότητες των δύο χωρών έχουν να κάνουν με αυτές ακριβώς τις ανάγκες.

Μεγάλη Βρετανία: Το εθνικό σύστημα της Μεγάλης Βρετανίας (National Health System-NHS) έχει θέσει έναν αριθμό από κατευθυντήριες γραμμές για την εθνική ασφάλεια και την πρόσβαση

στα δεδομένα ώστε να εξασφαλίζεται ότι οι πληροφορίες που είναι αποθηκευμένες σε υπολογιστές προστατεύονται από παραβιάσεις του απορρήτου, αλλοίωση ή παραφθορά καθώς και απώλεια. Υπάρχουν συγκεκριμένες υποχρεώσεις νομικά κατοχυρωμένες για να διαφυλάξουν την πληροφορία η οποία διαφυλάσσεται σε υπολογιστές του NHS όπως το Data Protection Act και Computer Misuse Act.

Το υπουργείο υγείας έχει συμβουλέψει για το ποιες είναι οι κατευθυντήριες γραμμές ώστε να εξασφαλιστεί το ιατρικό απόρρητο προσωπικών ιατρικών δεδομένων. Υπάρχουν δημοσιεύσεις διαθέσιμες για να βοηθήσουν την επιθεώρηση των κανονισμών που έχουν να κάνουν με την ασφάλεια, στις οποίες συμπεριλαμβάνεται η πολιτική ασφάλειας που ακολουθεί το ίδιο το NHS για δίκτυα υπολογιστών καθώς και ο οδηγός ασφάλειας IM&T. Με τον ίδιο τρόπο μπορεί να ελεγχθεί και η συμμόρφωση με το Data Protection Act.

ΗΠΑ: Το American Society for Testing and Materials – ASTM μέσω των υποεπιτροπών του δραστηριοποιείται σε ανάλογα ζητήματα. Συγκεκριμένα, η υποεπιτροπή E31.12 του ASTM για τον ιατρικό φάκελο Ασθενή έχει αναπτύξει το «Guidelines for minimal Data Security Measures for the Protection of Computer-Based Patient Records». Επίσης, Η υποεπιτροπή E31.17 του ASTM εργάζεται πάνω σε πρότυπα για την πρόσβαση και το απόρρητο των Ιατρικών Φακέλων, ενώ Η υποεπιτροπή E31.20 του ASTM έχει αναπτύξει τις προδιαγραφές που πρέπει να έχουν τα πρότυπα για τον έλεγχο της πρόσβασης στην ιατρική πληροφορία.

2.4 Γιατί απαιτούνται οι ιατρικές κωδικοποιήσεις στα Πληροφοριακά Συστήματα Υγείας

Η χρήση κωδικοποιήσεων στα Πληροφοριακά Συστήματα Υγείας δίνει τη δυνατότητα για συστηματική, τυποποιημένη και αξιοποιήσιμη καταγραφή πληροφοριών που επιτρέπει την ορθολογική ανάπτυξη και τήρηση ιατρικού ιστορικού, την υποστήριξη της διάγνωσης και τη γενικότερη αναβάθμιση της υγειονομικής περίθαλψης. Επιτρέπει επίσης στον ερευνητή και στατιστικολόγο να προβεί σε ενδελεχείς αναλύσεις και συγκρίσεις δεδομένων με στόχο τη τήρηση ουσιαστικών και πραγματικών στατιστικών δεδομένων που αφορούν στη Δημόσια Υγεία ενός Κράτους.

Επίσης η χρήση κωδικοποιήσεων επιτρέπει στο διοικητικό προσωπικό και τη διοίκηση των μονάδων υγείας να πετύχουν τον βέλτιστο επιμερισμό του κόστους ανά ιατρική πράξη για παράδειγμα, ενώ επιτρέπει τον σωστό προγραμματισμό των προμηθειών και την εξασφάλιση των αναγκαίων πόρων προκειμένου να επιτευχθούν οι απαιτούμενοι στρατηγικοί στόχοι. Σε επίπεδο Πολιτικής Ηγεσίας, οι κωδικοποιήσεις επιτρέπουν την ορθή τεκμηρίωση και λήψη αποφάσεων που επηρεάζουν την Εθνική Πολιτική Υγείας και Πρόνοιας αλλά και δημιουργούν τις συνθήκες για την εναρμόνιση με τα Ευρωπαϊκά πρότυπα και οδηγίες.

Επιπλέον, σε κλινικό επίπεδο η χρήση δομημένων κωδικοποιήσεων επιτρέπει την ενίσχυση της ποιότητας διαγνώσεων, τη μείωση του χρόνου αναμονής του Πολίτη κατά τη παροχή υπηρεσιών ιατρικής περίθαλψης, την εργασιακή ικανοποίηση του εμπλεκόμενου προσωπικού λόγω του συστηματοποιημένου τρόπου εργασίας, την ενίσχυση της ιατρικής έρευνας (διεθνή και εθνική) και τη δραστική μείωση ιατρικών σφαλμάτων. Στη πράξη οι κωδικοποιήσεις διευκολύνουν στην αναζήτηση πληροφοριών και στη διάδοση της ιατρικής γνώσης, ενώ είναι απαραίτητες για την ανάπτυξη ενός επιτυχούς πλαισίου διαλειτουργικότητας μεταξύ των πληροφοριακών συστημάτων.

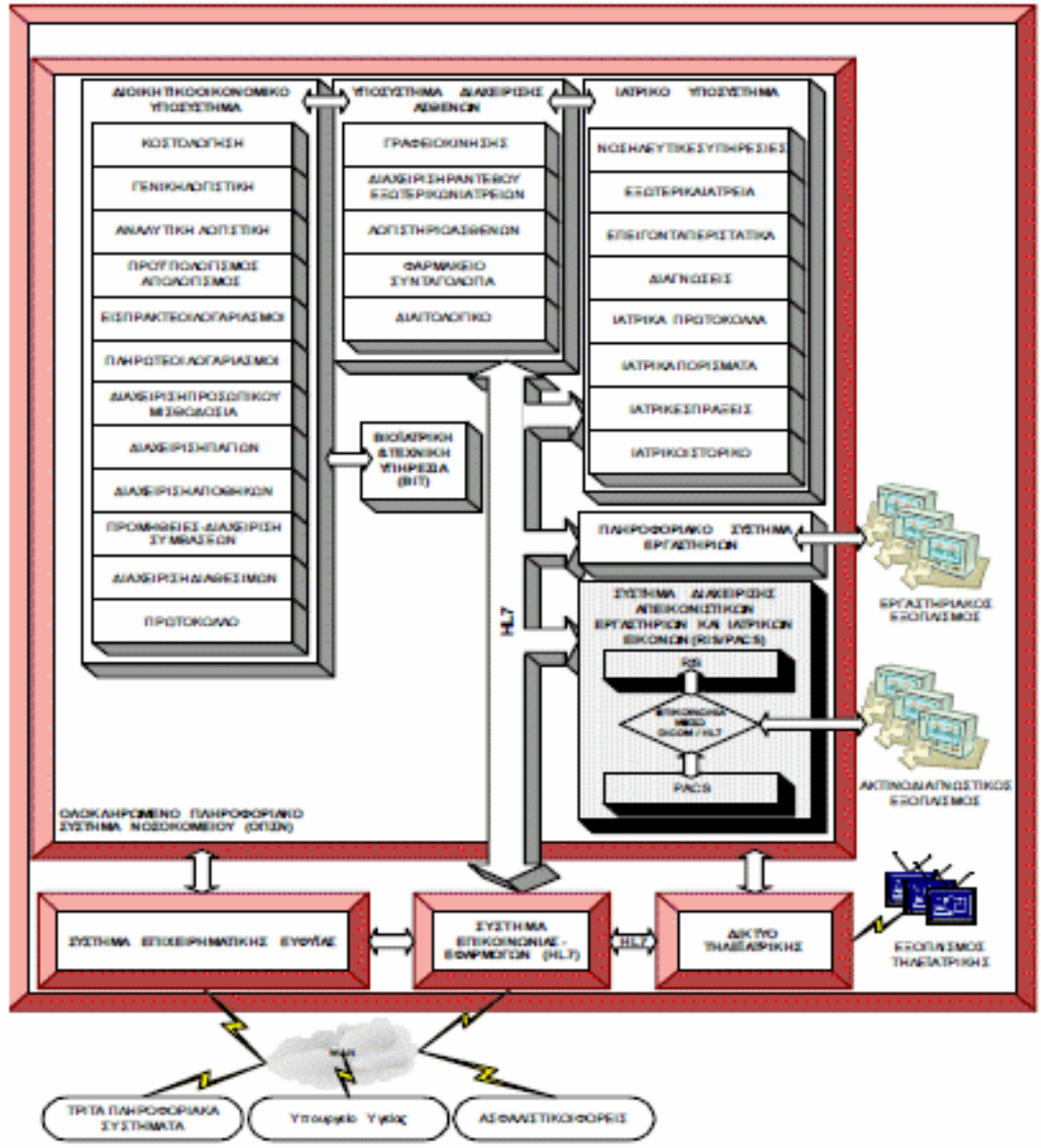
Ακόμα, έχει αναγνωριστεί διεθνώς ότι η χρήση πληροφοριακών συστημάτων κατά τη φάση της συνταγογράφησης φαρμάκων, όπως για παράδειγμα συστήματα ηλεκτρονικής συνταγογράφησης (e-prescribing), ηλεκτρονικής παραγγελίας (computer based patient order entry), χρήση εφαρμογών γραμμωτού κώδικα και άλλων, έχουν σημαντικά μειώσει τον αριθμό των λαθών. Στην Ιταλία για παράδειγμα, κάθε χρόνο εκτιμάται ότι χάνουν τη ζωή τους 14.000 ασθενείς από ιατρικά λάθη. Στις Η.Π.Α. πεθαίνουν κάθε χρόνο περισσότεροι άνθρωποι (από 44.000 μέχρι και 98.000 ανάλογα με τις δημοσιευμένες μελέτες) από ιατρικά λάθη παρά από τροχαία, από καρκίνο του μαστού, από το AIDS, κ.λπ. Όλες οι μελέτες δίνουν έμφαση στο γεγονός ότι πολλά ιατρικά λάθη αλλά και θάνατοι θα μπορούσαν να αποφευχθούν αν μπορούσαν να συλλέγονται αξιόπιστα ιατρικά δεδομένα για αυτά, ώστε να αποκαλύπτονται τα αίτια. Τα παραπάνω σχετίζονται άμεσα με την έλλειψη χρήσης κωδικοποιημένων στοιχείων.

Η χρήση κωδικοποιήσεων στα πληροφοριακά συστήματα στην Υγεία και Πρόνοια δίνει τη δυνατότητα σε αυτά να δια-λειτουργούν αποτελεσματικά, να ανταλλάσσουν δεδομένα, και να δημιουργήσουν στο μέλλον τον ολοκληρωμένο Ηλεκτρονικό Φάκελο Υγείας του Πολίτη, συνδυάζοντας τα αναγκαία και χρήσιμα δεδομένα από όλα τα περιστατικά (patient encounters) επαφής ενός ασθενή με το εκάστοτε σύστημα υγείας. Η δημιουργία ενός παρόμοιου φακέλου δεν είναι εφικτός χωρίς τη χρήση κωδικοποιήσεων οι οποίες είναι κατανοητές και αξιοποιήσιμες από όλους του εξουσιοδοτημένους από τον Πολίτη - κάτοχο αναγνώστες του φακέλου αυτού. Οι κωδικοποιήσεις δηλαδή δημιουργούν τις ιδανικές συνθήκες για τη επίτευξη της σημασιολογικής διαλειτουργικότητας (semantic interoperability).

Είναι προφανές ότι η χρήση κωδικοποιήσεων στον τομέα υγείας αποτελεί ένα απαραίτητο εργαλείο και μέσο για την βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών και την εισαγωγή και ανάπτυξη πληροφοριακών συστημάτων. Η πρωτοβάθμια φροντίδα υγείας (ΠΦΥ) αποτελεί ένα σημαντικό τομέα στον οποίο αντιμετωπίζονται προβλήματα υγείας, συχνά εκφραζόμενο με διαφορετική εικόνα και συμπτωματολογία από ότι τα αντίστοιχα στο νοσοκομειακό τομέα. Η ανάπτυξη ολοκληρωμένων πληροφοριακών συστημάτων απαιτεί ενιαίες κωδικοποιήσεις και αντιστοίχηση όρων και πρακτικών μεταξύ πρωτοβάθμιας και νοσοκομειακής φροντίδας.

2.5 Διασύνδεση Νοσοκομειακών Πληροφοριακών Συστημάτων

Τα νοσοκομεία αποτελούν ένα μέρος του Συστήματος Υγείας και Πρόνοιας το οποίο περιλαμβάνει ακόμα την πρόληψη, τη πρωτοβάθμια περίθαλψη, τη νοσηλεία στο σπίτι, τη κοινωνική ασφάλιση και την ιατρική έρευνα. Τα νοσοκομεία είναι ο ακρογωνιαίος λίθος ο οποίος στηρίζει την ομαλή λειτουργία του Συστήματος Υγείας. Η ταχύτητα που απαιτείται σήμερα στη λήψη σωστών αποφάσεων, επιβάλλει τη μηχανογράφηση του Συστήματος Υγείας και Πρόνοιας και κατ' επέκταση και του νοσοκομειακού κλάδου (McKee & Healy, 2002). Η μηχανογράφηση ενός νοσοκομείου είναι μια περίπλοκη διεργασία η οποία απαιτεί τη διασύνδεση ανομοιογενών τμημάτων τα οποία ανταλλάσσουν πληροφορίες προς όφελος του Πολίτη. Ένα ολοκληρωμένο πληροφοριακό σύστημα νοσοκομείου (ΟΠΣΝ) ή Hospital Information System (HIS) αποτελείται από μια πληθώρα υποσυστημάτων. Τα κύρια υποσυστήματα φαίνονται στο Σχήμα 2.3



Σχήμα 2.3 *Ενδεικτική διάταξη υποσυστημάτων HIS*

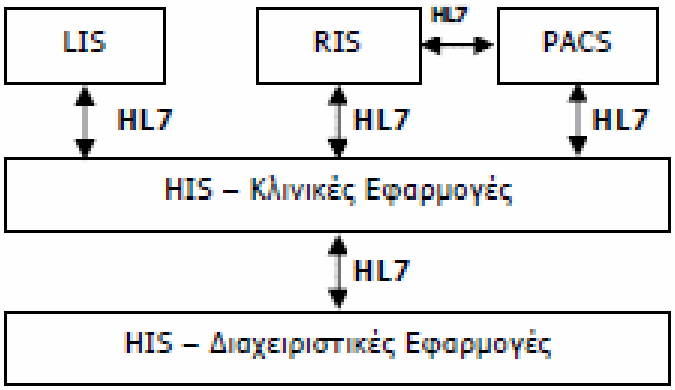
Η μηχανογράφηση των νοσοκομείων έχει μόνο θετικά στοιχεία να προσφέρει. Η εγκατάσταση και λειτουργία ενός HIS προσβλέπει στη βελτίωση των συνθηκών νοσηλείας, στη μείωση του κόστους λειτουργίας και στην αυτοματοποίηση των διαδικασιών.

Προκειμένου να είναι σε θέση η διοίκηση ενός νοσοκομείου να παρακολουθεί με πραγματικά στοιχεία τη λειτουργία του απαιτείται η εξαγωγή έγκυρων δεδομένων σε μορφή επεξεργασμένης πληροφορίας (αναφορές, εκτυπώσεις καθημερινής εργασίας, στατιστικά δεδομένα, δείκτες ποιότητας, δείκτες αποτελεσματικότητας, δείκτες υγείας, κ.λπ.). Έτσι η διοίκηση ενός νοσοκομείου στηρίζεται στις πληροφορίες που αντλεί από τα συνεργαζόμενα συστήματα που υπάρχουν στο νοσοκομείο και συνεπώς όσο πληρέστερη είναι η ανάπτυξη της πληροφοριακής

υποδομής τόσο ευκολότερο είναι το έργο της διοίκησης μιας μονάδας υγείας. Τα παρακάτω πληροφοριακά συστήματα βελτιστοποιούν τη λειτουργία ενός νοσοκομείου:

- Το Πληροφοριακό Σύστημα Εργαστηρίων (ΠΣΕ, ή LIS – Laboratory Information System)
- Το Πληροφοριακό Σύστημα Ακτινολογικών Εξετάσεων (RIS – Radiology Information System)
- Το Σύστημα Αρχειοθέτησης και Επικοινωνίας Ιατρικών Εικόνων (PACS – Picture Archiving and Communication system)
- Διάφορα συστήματα Τηλεϊατρικής και κατ' οίκον νοσηλείας

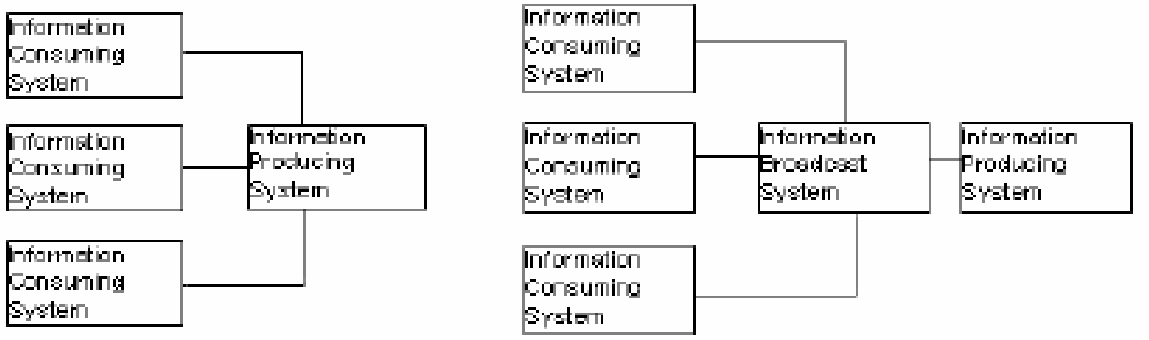
Όπως έχει γίνει σαφές στις προηγούμενες παραγράφους, η δημιουργία πληροφοριακών υποδομών ακόμα και εντός ενός νοσοκομείου, πόσο μάλλον μεταξύ μονάδων υγείας είναι μια σύνθετη διαδικασία που δεν μπορεί να καλυφθεί από μία και μόνο εφαρμογή λόγω της πολυπλοκότητας του χώρου της υγείας και πρόνοιας. Κατά συνέπεια απαιτείται η δημιουργία ενός πλαισίου διαλειτουργικότητας βασισμένο σε διεθνή πρότυπα και πρακτικές. Παρακάτω περιγράφεται η βέλτιστη τεχνική λύση για τη δημιουργία ενός τέτοιου πλαισίου. Στη λύση αυτή, όλα τα συστήματα συνδέονται μέσω ενός υποσυστήματος διασύνδεσης HL7 (middleware), με μια κοινή υποδομή επικοινωνίας (Common Communication Infrastructure - CCI). Αυτή η υποδομή επικοινωνίας φροντίζει όλες οι πληροφορίες που στέλνονται από ένα σύστημα να παραδίδονται στον προοριζόμενο παραλήπτη. Όταν αυτό είναι αδύνατο το CCI θα ενημερώνει το σύστημα αποστολής για την αποτυχία εκτέλεσης της παράδοσης. Το HL7 (Health Level 7) αναγνωρίζεται διεθνώς ως η πιο δόκιμη και πετυχημένη λύση στο πρόβλημα της διαλειτουργικότητας στο χώρο της υγείας (Spyrou & Berler & Bamidis, 2003) όπως περιγράφεται αναλυτικότερα και σε προηγούμενη ενότητα. Στο Σχήμα 2.4 απεικονίζονται οι βασικές ανάγκες διασύνδεσης εντός ενός νοσοκομείου.



Σχήμα 2.4 *Βασικές ανάγκες διασυνδεσιμότητας μεταξύ εφαρμογών σε ένα νοσοκομείο*

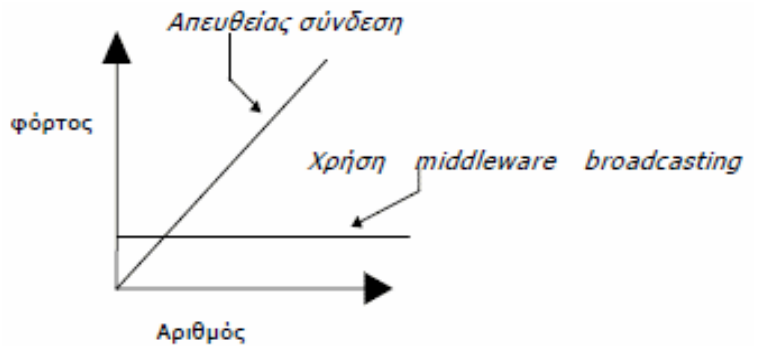
Ιδεωδώς όλα τα πληροφοριακά συστήματα κατανάλωσης είναι ικανά να λαμβάνουν πληροφορίες υπό τη μορφή μηνυμάτων (Application Protocol Data Units – APDUs).

Προκειμένου να φτάσουμε όσο το δυνατόν πιο κοντά σ' αυτήν την ιδανική κατάσταση χρησιμοποιείται ένα πρόσθετο σύστημα middleware που εκτελεί μια επαναλαμβανόμενη σύνδεση με την (τις) βάση (εις) δεδομένων και εξάγει τις πιο πρόσφατες πληροφορίες σε τακτά χρονικά διαστήματα (information broadcast system). Είναι έτσι το μόνο σύστημα που συνδέεται κατευθείαν με τη βάση δεδομένων που φέρει τις τρέχουσες πληροφορίες. Αυτό το σύστημα παράγει τα APDUs με τις πληροφορίες και τα μεταδίδει σε όλα τα συνδεδεμένα πληροφοριακά συστήματα. Το Σχήμα 2.5 παρουσιάζει την διαφορά μεταξύ της απευθείας διασύνδεσης με μια βάση δεδομένων (συνήθως με επιβάρυνση του φόρτου εργασίας της βάσης δεδομένων) και μέσω middleware.



Σχήμα 2.5 *Χρήση εφαρμογής τύπου middleware*

Η συνέπεια της εισαγωγής ενός middleware broadcasting system είναι ότι το φορτίο εργασίας στη βάση δεδομένων παραμένει σταθερό αντί να είναι ανάλογο με τον αριθμό των συνδεδεμένων πληροφοριακών συστημάτων. Αυτό είναι ιδιαίτερα σημαντικό και αφορά τα «κληροδοτημένα» (legacy) πληροφοριακά συστήματα τα οποία ήδη λειτουργούν στα όριά τους. Το παρακάτω διάγραμμα (Σχήμα 2.6) εικονογραφεί την επιβάρυνση του συστήματος.



Σχήμα 2.6 *Απλοποιημένη σχηματική αναπαράσταση της επιβάρυνσης πληροφοριακών συστημάτων*

Για να επιτευχθεί ευρεία μετάδοση (σε πολλούς αποδέκτες - εφαρμογές) των δεδομένων σε πραγματικό χρόνο, το middleware broadcasting system συνδέεται ανά τακτά χρονικά διαστήματα στην βάση δεδομένων σε βαθμό που του επιτρέπει να επιδεικνύει συμπεριφορά

πραγματικού χρόνου (real-time). Προφανώς όσο υψηλότερη είναι η συχνότητα τόσο επιβαρύνεται η βάση δεδομένων. Εδώ πάλι πρέπει να βρεθεί η χρυσή τομή μεταξύ υπερφόρτωσης και συμπεριφοράς σε πραγματικό χρόνο. Ο όρος «πραγματικός χρόνος» συχνά εννοείται σαν «πολύ γρήγορος σε απόκριση». Εντούτοις η σωστή ερμηνεία είναι «αρκετά γρήγορος για να κρατήσει πιστά την σειρά των σχετικών συμβάντων του πραγματικού κόσμου που το σύστημα παρακολουθεί». Για παράδειγμα, το γεγονός ότι ένας ασθενής έχει εισαχθεί, πρέπει να γίνει γνωστό στον θάλαμο διαμονής του πριν φτάσει ο ίδιος εκεί.

Η χρησιμοποίηση HL7 APDUs για ανταλλαγή πληροφοριών μεταξύ συστημάτων φέρει ορισμένα ξεχωριστά πλεονεκτήματα:

- Όλα τα συστήματα μπορούν να διασυνδεθούν μεταξύ τους με έναν κοινό τρόπο.
- Υπάρχει αποσύνδεση μεταξύ των συστημάτων η οποία επιτρέπει οι πληροφορίες να δρομολογούνται, να αποθηκεύονται, να προωθούνται, και να επεξεργάζονται ανεξάρτητα από την πραγματική ανταλλαγή.
- Τα πληροφοριακά συστήματα που ανταλλάσσουν πληροφορίες δεν χρειάζεται να αποκαλύπτουν την εσωτερική τους δομή το ένα στο άλλο. Αυτή η μορφή της «απόκρυψης των πληροφοριών» (information hiding) βελτιώνει σημαντικά την ικανότητα σύνδεσης των συστημάτων.

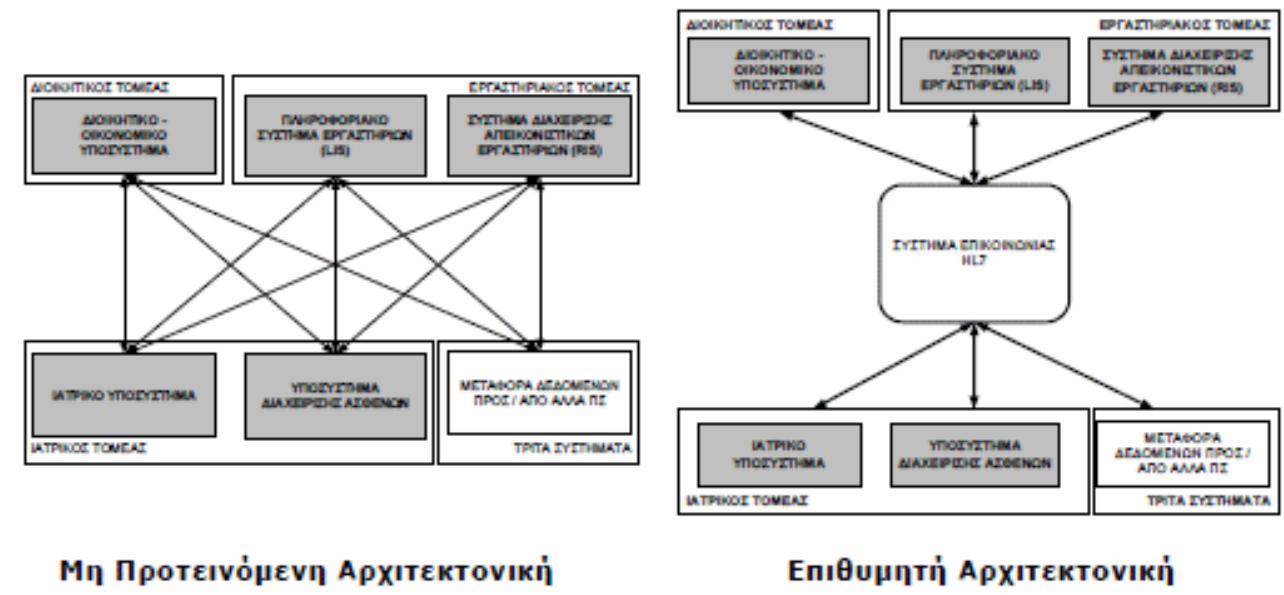
Όταν συστήματα παρέχουν μια κοινή διεπαφή (interface) για αποστολή και παραλαβή πληροφοριών όχι μόνο μπορούν εύκολα να συνδεθούν αλλά ακόμη κι η δρομολόγηση των πληροφοριών γίνεται εφικτή. Το τελευταίο είναι πολύ σημαντικό για την διασύνδεση απομακρυσμένου συστήματος που δεν μπορεί να επικοινωνήσει κατ' ευθείαν.

Η πιο δόκιμη αντιμετώπιση είναι η χρήση τεχνολογιών ανταλλαγής μηνυμάτων (messaging) που είναι ευρέως διαδεδομένες και εύκολο να αναπτυχθούν (Grimson, 2000). Η βασική ιδέα είναι η χρήση μιας αρχιτεκτονικής ανταλλαγής μηνυμάτων από τους διάφορους εμπλεκόμενους χρήστες σε μία διαδικασία, και στην αυστηρή τυποποίηση των μηνυμάτων. Η αρχιτεκτονική κατανεμημένων πληροφοριακών συστημάτων που διαλειτουργούν μεταξύ τους (federated information systems) πρέπει να λαμβάνει υπόψη την υφιστάμενη κατάσταση εφαρμογών που συχνά είναι ήδη αποδεκτές από τους χρήστες. Σε ότι αφορά την διατηρησιμότητα υφιστάμενων εφαρμογών πρέπει κανείς να λάβει υπόψη ότι:

- Πολλά από τα ήδη υπάρχοντα συστήματα δεν χρειάζεται να αλλαχτούν (καλύπτουν λειτουργικές ανάγκες και χρησιμοποιούνται από τους χρήστες).
- Κανένα σημαντικό πρόσθετο φορτίο (workload) δεν πρέπει να εισάγεται στα ήδη υπάρχοντα συστήματα λόγω της διασύνδεσης τους.
- Η διασύνδεση των υπαρχόντων συστημάτων πρέπει να είναι μια οικονομικώς συμφέρουσα ενέργεια.

Έτσι, η αντικατάσταση υφιστάμενων πληροφοριακών συστημάτων μιας μονάδας υγείας μπορεί να αποφεύγεται κατά το δυνατόν με τη χρήση του προτύπου HL7 ως μέσο ανταλλαγής δεδομένων όπου αυτό είναι εφικτό. Δεν πρέπει να λαμβάνεται υπ' όψιν μόνο το κόστος αγοράς ενός καινούργιου συστήματος. Τα κρυφά κόστη είναι συνήθως πολύ υψηλότερα (εκπαίδευση, μεταφορά δεδομένων, κ.λπ.). Το γεγονός ότι η διεπαφή (interface) με ένα πληροφοριακό σύστημα δεν είναι πάντα εύκολη, δεν είναι ικανός λόγος για την αντικατάσταση του πληροφοριακού συστήματος (deinvestment). Μόνο συστήματα βασισμένα σε απαρχαιωμένη ή περιοριστική τεχνολογία, ή με τεχνολογικές και λειτουργικές ελλείψεις (γραφικό περιβάλλον, περιορισμένη κάλυψη των διαδικασιών, κ.λπ.) πρέπει απαραίτητα να αντικαθιστώνται.

Είναι λοιπόν προφανές ότι χωρίς την χρήση του προτύπου HL7 υφίσταται η αναγκαιότητα κατασκευής και υποστήριξης πολλών διεπαφών διαφορετικού τύπου. Πέραν του πλήθους των διεπαφών που πρέπει να κατασκευασθούν και να προσαρμοσθούν, η διαχείριση της διαδικασίας γίνεται δύσκολη διότι απαιτείται οι συνεργασία ανά δύο των κατασκευαστών των διαφόρων συστημάτων. Με την χρήση ενός υποσυστήματος διασύνδεσης μέσω HL7 (middleware) η κατάσταση διαμορφώνεται όπως φαίνεται στο Σχήμα 2.7. Σε αυτήν την περίπτωση υλοποιούνται λιγότερες διεπαφές.



Σχήμα 2.7 *Απλοποιημένη σχηματική αναπαράσταση της μείωσης των αναγκαίων διεπαφών*

Κατά τη διάρκεια των προηγούμενων δεκαετιών ο οργανισμός HL7 προσδιόρισε έναν μεγάλο αριθμό προτύπων που στοχεύουν στην διευκόλυνση των προμηθευτών και των χρηστών στη διασύνδεση των εφαρμογών στην υγειονομική περίθαλψη. Τα πρότυπα αυτά εφαρμόζονται στην υγειονομική περίθαλψη διεθνώς. Σκοπός της εξέλιξης του προτύπου είναι να εκφρασθούν ρητά οι διαφορετικές ερμηνείες που υφίστανται κατά την εφαρμογή των προτύπων, αναμένοντας ως συνέπεια μια περαιτέρω μείωση του κόστους της διαλειτουργικότητας. Για τον λόγο αυτό έχει

υπάρξει ιδιαίτερο ενδιαφέρον για τον έλεγχο της συμμόρφωσης με τα πρότυπα αυτά. Ο μηχανισμός συμβατότητας που προτείνεται από τον οργανισμό HL7 και συγκεκριμένα την ειδική ομάδα ενδιαφέροντος της συμβατότητας (SIG Conformance) είναι τα προφίλ συμμόρφωσης τα οποία αναλύονται σε μια τυποποιημένη δήλωση συμμόρφωσης (conformance statement). Η εφαρμογή αυτών των προφίλ συμμόρφωσης στην Ελλάδα αποτελεί την μοναδική ίσως δυνατότητα εισαγωγής και υλοποίησης του προτύπου HL7 με τρόπο οργανωμένο και με προοπτική δημιουργίας της κατάλληλης κουλτούρας μεταξύ των εμπλεκόμενων φορέων (Μονάδες Υγείας και Πρόνοιας, Συναρμόδια Υπουργεία, Εταιρίες Πληροφορικής, επιστημονική Κοινότητα, κ.λπ.).

2.6 Απαιτήσεις Ασφάλειας για Διασυνδεδεμένα Συστήματα Υγείας

Τα πρότυπα ιατρικής πληροφορίας παρέχουν το βασικό πλαίσιο ανάπτυξης ισχυρών διασυνδεδεμένων εφαρμογών υγείας. Παρόλα αυτά, η ασφαλής ανταλλαγή και αποδέσμευση ηλεκτρονικών αρχείων υγείας (EHR-electronic health records) μέσω επισφαλών καναλιών όπως το διαδίκτυο, απαιτεί την εφαρμογή περιεκτικών τεχνολογιών ασφάλειας που επιτρέπουν την ανταλλαγή δεδομένων (Choe & Yoo, 2008). Οι τεχνολογίες ασφάλειας οφείλουν να παρέχουν μηχανισμούς για τον έλεγχο πρόσβασης και να ορίζουν προνόμια πρόσβασης για την προστασία των δεδομένων, της ιδιωτικότητας και την διαχείριση της πληροφορίας (Blobel et al., 2006; Ohno - Machadoa et al., 2004). Τα ευαίσθητα δεδομένα του ασθενή πρέπει πάντα να προστατεύονται κατά την ηλεκτρονική ανταλλαγή ιατρικών δεδομένων. Η μη εξουσιοδοτημένη πρόσβαση και η αποδέσμευση ευαίσθητων πληροφοριών θεωρούνται παραβίαση της εμπιστευτικότητας και μπορούν να οδηγήσουν σε ζητήματα δημοσίου ενδιαφέροντος όπως ρατσισμό, αμηχανία ή οικονομική καταστροφή (Ohno - Machadoa et al., 2004). Σε αυτό το σημείο, πρέπει να ληφθούν υπόψη τα εξής ζητήματα:

- Προέλευση της πληροφορίας
- Αιτία αποκάλυψης της πληροφορίας και προορισμός της
- Ασφαλής μετάδοση των δεδομένων
- Προστασία της ιδιωτικότητας του ασθενή

Πίνακας 2.1 *Σύνοψη των απαιτήσεων επικοινωνίας και ασφάλειας*

	Τοπική	Ενδο-οργανική
Βασική	• Τυποποιημένες διεπαφές λογισμικού πεδίου • Τυποποιημένοι ορισμοί μηνυμάτων	• Τυποποιημένες διεπαφές λογισμικού πολλαπλών πεδίων • Τυποποιημένοι ορισμοί μηνυμάτων

	πεδίου • Εισαγωγή / εξαγωγή λειτουργιών για συμβατές εφαρμογές • Τοπικές πολιτικές πρόσβασης και ασφάλειας • Role-based πολιτικές ελέγχου πρόσβασης • Τοπική ασφάλεια επικοινωνιών • Ασφάλεια εφαρμογών (διαθεσιμότητα, αναγνώριση, ακεραιότητα δεδομένων, υπευθυνότητα και ιχνηλασιμότητα)	πολλαπλών πεδίων • Τυποποιημένες πολιτικές πρόσβασης και ασφάλειας • Κοινοί ορισμοί για role-based πολιτικές ελέγχου πρόσβασης • Συμφωνίες πολιτικών πρόσβασης και ασφάλειας • Ασφάλεια επικοινωνίας μεταξύ πεδίων (Εξουσιοδότηση και έλεγχος πρόσβασης, εμπιστευτικότητα, ακεραιότητα δεδομένων, υπευθυνότητα και ιχνηλασιμότητα)
Δευτερογενής	• Δυνατότητα αμφισβήτησης και ανωνυμίας των ηλεκτρονικών αρχείων υγείας • Πολιτικές ασφάλειας για δευτερογενής αποδέσμευση και χρήση των ηλεκτρονικών αρχείων υγείας (EHR) • Πολιτικές ασφάλειας για αποδέσμευση και χρήση των ηλεκτρονικών αρχείων υγείας (EHR) τρίτων • Τοπική ασφάλεια εφαρμογών και επικοινωνίας	• Ενσωμάτωση δεδομένων, δυνατότητα αμφισβήτησης και ανωνυμίας των διαδεδομένων ηλεκτρονικών αρχείων υγείας (EHR) • Κοινές πολιτικές και πολιτικές συμφωνίας για πρόσβαση και αποδέσμευση για δευτερογενή χρήση των ηλεκτρονικών αρχείων υγείας (EHR) • Κοινές πολιτικές και πολιτικές συμφωνίας για αποδέσμευση / χρήση ηλεκτρονικών αρχείων υγείας (EHR) τρίτων • Ενδο-πεδιακή εφαρμογή και ασφάλεια επικοινωνιών

Η προέλευση της επικοινωνίας αναφέρεται στο ποιος και πού έχουν συλλεχθεί τα δεδομένα. Η ιατρική πληροφορία μπορεί να συλλέγεται από διαφορετικούς οργανισμούς, να εξυπηρετεί μια πληθώρα σκοπών και η αποθήκευσή της μπορεί να είναι τοπική ή εξωτερική. Η τοπικά αποθηκευμένη πληροφορία μπορεί να είναι άμεσα διαθέσιμη και ο χρήστης μπορεί να έχει πρόσβαση σε αυτή σε οποιοδήποτε χρόνο και από οποιαδήποτε θέση μέσα στον οργανισμό. Σε αντίθεση, τα εξωτερικά ιατρικά δεδομένα ανακτούνται, συνήθως, από πληροφοριακά συστήματα που δεν παρέχουν δικαιώματα άμεσης πρόσβασης στον χρήστη. Στην περίπτωση αυτή, τα

δικαιώματα πρόσβασης που παρέχονται βασίζονται σε κοινές συμφωνίες μεταξύ των συμβαλλόμενων οργανισμών (Lopez & Blobel, 2009; van der Linden, et al.,2009).

Η αιτία της αποδέσμευσης των πληροφοριών είναι ένα σημαντικό στοιχείο για τον καθορισμό μιας αποτελεσματικής στρατηγικής ασφάλειας. Για την υποστήριξη βασικών υπηρεσιών όπως η θεραπεία ενός υποκειμένου υγείας, συνήθως, απαιτείται λεπτομερής πληροφόρηση. Αντιθέτως, οι πληροφορίες που απαιτούνται για δευτερογενείς χρήσεις δεν θα πρέπει να συνδέονται με τον ασθενή (Agrawal & Johnson,2007). Ο προορισμός της πληροφορίας επηρεάζει επίσης τον καθορισμό μιας στρατηγικής ασφάλειας. Οι ανάγκες τοπικής ασφάλειας διαφέρουν ουσιαστικά από τις απαιτήσεις ενός κατανεμημένου σεναρίου υγείας (van der Linden, et al.,2009). Σε τοπικό επίπεδο, πρότυπα μέτρα ασφάλειας και τυποποιημένα μηνύματα επιτρέπουν την ασφαλή πρόσβαση και αποδέσμευση πληροφοριών. Παρόλα αυτά, η ασφαλής ανταλλαγή και αποδέσμευση πληροφοριών μεταξύ διαφορετικών οργανισμών, δεν στηρίζεται μόνο σε ασφαλείς και τυποποιημένους ηλεκτρονικούς μηχανισμούς αλλά και σε τυποποιημένες πολιτικές ασφάλειας και πρόσβασης (Lopez & Blobel, 2009;). Στην πραγματικότητα, διαφορετικά ιδρύματα υγείας πιθανόν να έχουν και διαφορετικές πολιτικές ασφάλειας, ειδικά όσον αφορά προνόμια πρόσβασης και αποδέσμευση ηλεκτρονικών αρχείων υγείας για βασικές και δευτερογενείς χρήσεις. Οι αντικρουόμενες πολιτικές ασφάλειας θα μπορούσαν να προκαλέσουν παραβίαση της ασφάλειας, της εμπιστευτικότητας και της ιδιωτικότητας των ιατρικών δεδομένων του ασθενή (Choe & Yoo, 2008). Ο πίνακας 2.1 παρουσιάζει συνοπτικά τις απαιτήσεις που πρέπει να ικανοποιηθούν ανάλογα με τη χρήση και τον προορισμό της πληροφορίας. Στις επόμενες παραγράφους παρουσιάζεται μια πιο λεπτομερή ανάλυση των τμημάτων του πίνακα 2.1.

2.6.1 Τοπική Ανταλλαγή Δεδομένων και Ασφάλεια για Βασική Χρήση Πληροφοριών

Ως βασικό στοιχείο για την υποστήριξη δραστηριοτήτων υγειονομικής περίθαλψης θεωρούνται οι τοπικές εφαρμογές ηλεκτρονικών αρχείων υγείας (EHRs). Συγκεκριμένα, μειώνουν το κόστος, βελτιώνουν την ποιότητα των υπηρεσιών, ενισχύουν την διανομή υγειονομικής περίθαλψης και υποστηρίζουν την βασική και δευτερογενή χρήση των πληροφοριών. Προκειμένου να διευκολυνθεί η πρόσβαση σε τοπικά αποθηκευμένες πληροφορίες, τα πληροφοριακά συστήματα υγείας οφείλουν να είναι διαλειτουργικά με ασφαλή τρόπο. Γενικά, οι τοπικές εφαρμογές ηλεκτρονικών αρχείων υγείας θα πρέπει να λαμβάνουν υπόψη την ύπαρξη ετερογενών πηγών πληροφορίας, τις απαιτήσεις ασφάλειας για την προστασία των ιατρικών δεδομένων του ασθενή και την εφαρμογή πολιτικών ασφάλειας για την πρόσβαση και αποδέσμευση δεδομένων.

Η ύπαρξη ετερογενών πληροφοριακών συστημάτων υγείας (ΠΣΥ) έχει εγείρει ζητήματα που αφορούν την διαλειτουργικότητα και συμβατότητα ιατρικών αρχείων και έχει περιορίσει την συλλογή ολοκληρωμένων, ιατρικών πληροφοριών του ασθενή από τοπικές αρχιτεκτονικές πληροφοριών (Coonan, 2004). Η ανάπτυξη μιας επαρκούς υποδομής υγειονομικής περίθαλψης

οφείλεται στην ενσωμάτωση των ιατρικών προτύπων πληροφορικής (Hammond, 1995; Hammond & Cimino, 2001), με την οποία μπορεί να ξεπεραστεί ο περιορισμός που παράγεται από την υιοθέτηση ετερογενών πληροφοριακών συστημάτων. Η επικοινωνία και η διαλειτουργικότητα των ΠΣΥ καθώς και η παροχή πρόσβασης σε ηλεκτρονικά αρχεία υγείας (ΗΑΥ), διευκολύνεται από τυποποιημένες διεπαφές λογισμικού πεδίου, τυποποιημένους ορισμούς μηνυμάτων πεδίου και την εισαγωγή / εξαγωγή λειτουργιών για συμβατές εφαρμογές.

Οι απαιτήσεις ασφάλειας για την πρόσβαση και προστασία των ιατρικών πληροφοριών των ασθενών, είναι επίσης κρίσιμοι παράγοντες για την ολοκλήρωση τοπικών αρχιτεκτονικών πληροφοριών υγείας. Η τοπική επικοινωνία και η ασφάλεια εφαρμογών πρέπει να εξασφαλίζουν διαθεσιμότητα των πληροφοριών, εμπιστευτικότητα, ταυτοποίηση και αυθεντικοποίηση του χρήστη, ακεραιότητα δεδομένων, υπευθυνότητα και ιχνηλασιμότητα των προσβάσιμων πληροφοριών. Η διαθεσιμότητα των πληροφοριών είναι ένα επίσης σημαντικό στοιχείο για την απόκτηση λειτουργικών συστημάτων ηλεκτρονικών αρχείων υγείας. Στους χρήστες με δικαιώματα πρόσβασης σε πληροφορίες, θα πρέπει να τους επιτρέπεται η πρόσβαση σε αυτές, προκειμένου να εκτελούν τα καθήκοντά τους (Blobel, 2004; Garson & Adams, 2008). Καθώς η πληροφορία τυχαίνει να γίνεται όλο και πιο διαθέσιμη σε όλους τους χρήστες στα όρια ενός οργανισμού, η ανησυχία για την προστασία της ιδιωτικότητας των ασθενών θεωρείται σημαντικός παράγοντας που οδηγεί στην εφαρμογή μέτρων ασφάλειας (Anderson, 2007; Blobel, 2006a). Η ακεραιότητα, η αξιοπιστία και η υπευθυνότητα είναι επίσης σημαντικές απαιτήσεις που ένα ΠΣΥ πρέπει να ικανοποιεί, προκειμένου να διασφαλίζεται η διατήρηση μιας ασφαλούς πλατφόρμας ΗΑΥ.

Υπό αυτές τις προϋποθέσεις, κρίσιμο έργο για την ασφάλεια των ΗΑΥ είναι η διοίκηση των υπηρεσιών ασφάλειας και η ανάθεση δικαιωμάτων πρόσβασης (Blobel, 2004). Συνεπώς, είναι κρίσιμη η ακριβής αυθεντικοποίηση του χρήστη καθώς και η σωστή ανάθεση προνομίων πρόσβασης προκειμένου να διασφαλιστεί ότι η πρόσβαση, η πρόσθεση και η μετατροπή πληροφοριών γίνεται μόνο από άτομα που έχουν δικαίωμα να εκτελούν τέτοιες δραστηριότητες (Blobel, 2004). Το μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους (role-based access control – RBAC) έχει παρουσιαστεί ως η κατάλληλη λύση για την παροχή δικαιωμάτων πρόσβασης στις πληροφορίες του ασθενή. Το μοντέλο αυτό (RBAC) παρέχει μια λύση για την έμμεση ανάθεση δικαιωμάτων πρόσβασης βασισμένη στο ρόλο του ατόμου εντός του οργανισμού (Blobel, 2004), αλλά επίσης επιτρέπει την προσαρμογή των προνομίων πρόσβασης στους χρήστες, υπό συγκεκριμένες συνθήκες (Peleg, Beimel, Dori & Denekamp, 2008). Τα οφέλη και οι περιορισμοί του RBAC μοντέλου θα αναλυθούν σε επόμενο κεφάλαιο.

Η πρόσβαση πεδίου (domain) και υπό-πεδίου (sub-domain) και οι πολιτικές ασφάλειας θα πρέπει να καλύπτουν την νομοθεσία και τους κανονισμούς που αφορούν την μυστικότητα και την εμπιστευτικότητα των προσωπικών πληροφοριών, παρέχοντας ένα εσωτερικό κανονιστικό

πλαίσιο σχετικά με την αποδέσμευση πληροφοριών. Προκειμένου να αποφευχθεί η μη εξουσιοδοτημένη αποδέσμευση δεδομένων, τα ΠΣΥ πρέπει να παρέχουν μία υποδομή ασφάλειας η οποία να προστατεύει τις αρχές που εντάσσονται στο πλαίσιο των πολιτικών ασφάλειας του οργανισμού (Agrawal & Johnson, 2007; Conrick & Newell, 2006; Lusignan, et al., 2007).

2.6.2 Ανταλλαγή Δεδομένων Αμοιβαίου Ενδιαφέροντος και Ασφάλεια για Βασική Χρήση Πληροφοριών

Η ηλεκτρονική ανταλλαγή ΗΑΥ απαιτεί αφενός την κοινή χρήση τυποποιημένων μηνυμάτων που διευκολύνουν την ανταλλαγή πληροφοριών μεταξύ ετερογενών ηλεκτρονικών πληροφοριακών συστημάτων και αφετέρου την χρήση αποτελεσματικών μοντέλων προστασίας δεδομένων, τα οποία πρέπει να εγκατασταθούν για να εξασφαλιστεί η εμπιστευτικότητα, η αξιοπιστία και η εγκυρότητα των πληροφοριών που ανταλλάσσονται (Blobel, et al., 2006; Choe & Yoo, 2008). Ακόμη και αν η ενσωμάτωση μέτρων ασφάλειας για την προστασία ανταλλαγής ΗΑΥ μπορεί να εγγυηθεί την μυστικότητα των πληροφοριών του ασθενή κατά την μεταβίβαση των δεδομένων, δεν δύναται όμως να εξασφαλίσει την διατήρηση της εμπιστευτικότητας στα τελικά σημεία επικοινωνίας. Ως αποτέλεσμα, κρίνεται απαραίτητο να ενσωματωθούν τυποποιημένοι ορισμοί μηνυμάτων, υπηρεσίες ασφάλειας, μηχανισμοί ασφάλειας και κοινές πολιτικές πρόσβασης και ασφάλειας για την προστασία της εμπιστευτικότητας των πληροφοριών του ασθενή σε ένα κοινόχρηστο περιβάλλον υγειονομικής περίθαλψης (Blobel, et al., 2006).

Σύμφωνα με τα προαναφερθέντα, τα ΠΣΥ απαιτούν την ικανότητα ανταλλαγής σχετικών δεδομένων προκειμένου να ασκηθούν οι θεραπείες ασθενών εντός του δικτύου υγείας. Σύμφωνα με τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization), ένα σύστημα τυποποιημένου ΗΑΥ θα πρέπει να περιλαμβάνει την ικανότητα ανταλλαγής ενός ολοκληρωμένου ΗΑΥ, ή μέρος αυτού, και να υποστηρίζει την σειριακή διάταξη βάσεων δεδομένων με τυποποιημένα μηνύματα και δομές δεδομένων. Επιπλέον, το σύστημα θα πρέπει να διευκολύνει την σημασιολογική ερμηνεία των συγχωνευμένων δεδομένων που προέρχονται από ένα εξαγόμενο ΗΑΥ, να περιλαμβάνει την υποστήριξη για τον έλεγχο της πορείας των διαδικασιών ανταλλαγής, να παρέχει κανόνες που καλύπτουν την ανταλλαγή ενός τμήματος του αρχείου και να επιτρέπει την σημασιολογική διαλειτουργικότητα κλινικών εννοιών (ISO/TC-215, 2004). Η ανταλλαγή ιατρικών πληροφοριών μπορεί να επιτευχθεί με την εισαγωγή/εξαγωγή αρχείων στην περίπτωση συμβατών εφαρμογών λογισμικού ή με την χρήση τυποποιημένων μηνυμάτων στο σενάριο της ταυτόχρονης χρήσης πλατφόρμων λογισμικού και προσεγγίσεων που αφορούν την δομή πληροφοριών (Danko, et al., 2003; Muller, et al., 2005). Όπως προαναφέρθηκε, το HL7, η ASTM International (American Society for Testing and Material) και η Ευρωπαϊκή Επιτροπή Τυποποίησης (CEN) έχουν προωθήσει τυποποιημένα πλαίσια και

ορισμούς μηνυμάτων που διευκολύνουν την ανάπτυξη διεπαφών λογισμικού για την ανταλλαγή ηλεκτρονικών ιατρικών πληροφοριών χρησιμοποιώντας δημόσια δίκτυα όπως το Διαδίκτυο (Blobel, 2006a; Mc Donald, Overhage, Dexter, Takesue, & Suico, 1998).

Στο σενάριο αμοιβαίου ενδιαφέροντος, η ευθύνη για την διατήρηση της εμπιστευτικότητας των πληροφοριών κατανέμεται μεταξύ των διαφορών οργανισμών που συμμετάσχουν στο δίκτυο υγείας. Η ευθύνη αυτή δεν πρέπει μόνο να ληφθεί υπόψη, αλλά επίσης να απεικονίζεται και στην δομή πληροφοριών υγείας που έχει επιλεγεί. Η ικανοποίηση των αναγκών εμπιστευτικότητας και ασφάλειας είναι ζωτικής σημασίας για τα συστήματα ΗΑΥ ώστε να παρέχεται ένα ασφαλές και αξιόπιστο περιβάλλον συνεργασίας και επικοινωνίας μεταξύ των παρόχων υγειονομικής περίθαλψης. Η ασφάλεια δεν αφορά μόνο τις υπηρεσίες που θα τεθούν σε εφαρμογή για την αποφυγή μιας μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες, αλλά και τους μηχανισμούς που θα χρησιμοποιηθούν για την προστασία των δεδομένων των ασθενών και την παρεμπόδιση μιας μη εξουσιοδοτημένης αποδέσμευσης πληροφοριών σε οποιοδήποτε σημείο του καναλιού επικοινωνίας (Blobel, 2000; Blobel, et al., 2006; Blobel & Roger-France, 2001).

Η ασφάλεια επικοινωνιών και η ασφάλεια εφαρμογών είναι δυο βασικά στοιχεία που χρήζουν ιδιαίτερη προσοχή όταν πρόκειται για μετάδοση ευαίσθητων πληροφοριών. Η ασφάλεια επικοινωνιών αφορά σε όλες τις συνιστώσες που απαιτούνται για μια ασφαλή ανταλλαγή δεδομένων μεταξύ εφαρμογών λογισμικού, ενώ η ασφάλεια εφαρμογών αναφέρεται στα μέτρα ασφάλειας που χρησιμοποιούνται από πληροφοριακά συστήματα προκειμένου να προστατευθούν οι πληροφορίες που περιέχονται σε βάσεις δεδομένων και σε έγγραφα. Για την προστασία των πληροφοριών κατά την διάρκεια της ανταλλαγής μπορεί να χρησιμοποιηθεί ένα σύνολο τυποποιημένων μηχανισμών και υπηρεσιών. Παρόλα αυτά, το κρίσιμο ζήτημα είναι το πώς θα διασφαλίσουμε την ασφαλή αποδέσμευση των πληροφοριών όταν φτάσουν στον προορισμό τους. Η ανταλλαγή των πληροφοριών απαιτεί επίσης την εκτίμηση των εφαρμόσιμων πολιτικών κοινού συμφέροντος για την χρήση και την αποκάλυψη ιατρικών πληροφοριών (Conrick, 2006; Safran, et al., 2007). Μολονότι η προστασία της εμπιστευτικότητας του ασθενή είναι ένα νομικό και ηθικό ζήτημα που υπάγεται σε ειδική νομοθεσία, η τεχνική διάστασή της εγείρει μια πρόκληση την οποία οι αλλαγές της τεχνολογίας δεν αντιμετωπίζουν πάντοτε με αυστηρότητα (Conrick & Newell, 2006). Ο προσωπικός χαρακτήρας και η ευαισθησία των αποθηκευμένων σε ΗΑΥ πληροφοριών θέτει την μελέτη των υπηρεσιών ασφάλειας απαραίτητη, οι οποίες επιτρέπουν την πρόσβαση σε εξουσιοδοτημένους χρήστες και ταυτόχρονα προστατεύουν την εμπιστευτικότητα των πληροφοριών του ασθενή (Blobel, et al., 2006; Blobel & Roger-France, 2001; Γκρίτζαλης & Λαμπρινουδάκης, 2004). Παρόλα αυτά, δεν είναι απλή υπόθεση να σχεδιαστούν και να εφαρμοστούν μέτρα ασφάλειας για την προστασία της εμπιστευτικότητας των ασθενών και ταυτόχρονα να διευκολυνθεί η επικοινωνία των πληροφοριών μεταξύ των επαγγελματιών υγείας (Agrawal & Johnson, 2007; Γκρίτζαλης &

Λαμπρινουδάκης, 2004). Σε αυτό το σημείο, τα προβλήματα που εγείρονται δεν συνδέονται αποκλειστικά με την σωστή ανάθεση προνομίων πρόσβασης στις μεταδιδόμενες πληροφορίες, αλλά και με την ανάπτυξη κοινών πολιτικών ή πολιτικών επίλυσης συγκρούσεων που επιτρέπουν την πρόσβαση σε εξουσιοδοτημένους χρήστες (Blobel, et al., 2006; Blobel & Roger-France, 2001; Γκρίτζαλης & Λαμπρινουδάκης, 2004).

Μια προτεινόμενη λύση από τους Agrawal & Johnson αναφέρεται στην χρήση μιας «κολλώδους πολιτικής» η οποία έχει εγκριθεί για την ανταλλαγή πληροφοριών. Η εγκεκριμένη πολιτική περιλαμβάνει την αρχική πολιτική ελέγχου πρόσβασης που επιβάλλεται επί των μεταφερόμενων δεδομένων (Agrawal & Johnson, 2007). Παρόλα αυτά, δεν απαιτείται μόνο η χρήση πολιτικών τυποποιημένων γλωσσών για την ορθή ερμηνεία των μεταφερόμενων πολιτικών, αλλά τίθεται και ένα δυσχερές ζήτημα όταν οι τοπικές πολιτικές έρχονται τελικά σε διαφωνία με μια εγκεκριμένη πολιτική. Επιπλέον, οι πολιτικές ελέγχου πρόσβασης και ιδιωτικότητας ρυθμίζονται από κάθε ίδρυμα χωριστά βάσει όχι μόνο των νομικών φορέων και των κανονισμών, αλλά και των ηθικών αρχών που διέπουν την κουλτούρα ενός οργανισμού (Choe & Yoo, 2008). Ο Blobel πρότεινε ένα μοντέλο πολιτικής πολλαπλών πεδίων στο οποίο ορίζονται κοινές συμφωνίες πολιτικής πεδίων. Οι συμφωνίες αυτές είναι ορισμοί πολιτικών που καθιερώνονται μεταξύ των οργανισμών υγείας για να διευθετήσουν τυχόν ανακρίβειες μεταξύ των πολιτικών κατά την ανταλλαγή πληροφοριών (Blobel, 2004). Σε αυτή την περίπτωση, η ερμηνεία της πολιτικής θα εξαρτάται από την σύνταξη, τη σημασιολογία, το λεξιλόγιο και την λειτουργία των πολιτικών που ίσως παρουσιάσουν προβλήματα όταν ανταλλάσσονται πληροφορίες μεταξύ πεδίων που δεν στηρίζονται σε παρόμοια τεχνολογική υποδομή και παρόμοιους ορισμούς πολιτικών (Blobel, 2000; Blobel, et al., 2006; Blobel & Roger-France, 2001). Απαραίτητα στοιχεία για την εφαρμογή της προσέγγισης αυτής είναι η κανονικοποίηση των πολιτικών καθώς και ένας κοινός ορισμός του λεξιλογίου και της ερμηνείας των πολιτικών. Παρόλα αυτά, δεν έχει οριστεί ένα επίσημο πλαίσιο για ορισμούς πολιτικών στον τομέα της υγειονομικής περίθαλψης (Γκρίτζαλης & Λαμπρινουδάκης, 2004). Ούτε η κανονικοποίηση ή/και η τυποποίηση των ορισμών πολιτικής δεν έχουν επίσημα προταθεί.

2.6.3 Ανταλλαγή Δεδομένων και Ασφάλεια για Δευτερογενή Χρήση Πληροφοριών

Οι δευτερογενείς πληροφορίες που αποκτούνται από ηλεκτρονικά ΠΣΥ δεν είναι μόνο χρήσιμες για την βελτίωση της διανομής υπηρεσιών υγείας, αλλά μπορούν επίσης να χρησιμοποιηθούν ως ιστορική πηγή ιατρικών δεδομένων για έρευνα και εκπαιδευτικούς σκοπούς (Haux, 2006b). Ωστόσο, καθώς τα δευτερογενή δεδομένα αποκομίζονται από τις ηλεκτρονικές πληροφορίες των ασθενών, η τυχόν αποδέσμευσή τους χωρίς την κατάλληλη προστασία για την ιδιωτικότητα και την εμπιστευτικότητα των ασθενών θα μπορούσε να οδηγήσει σε βλάβη των ατόμων. Συνεπώς, η οποιαδήποτε σύνδεση δεδομένων που ενδεχομένως μπορεί να οδηγήσει σε αναγνώριση

ασθενών θα πρέπει να αποφεύγεται προκειμένου να προστατευθεί η ιδιωτικότητα και η εμπιστευτικότητα των ατόμων. Η ασάφεια και η ανωνυμοποίηση των δεδομένων είναι οι βασικές αρχές για την προστασία της ιδιωτικότητας και της εμπιστευτικότητας των ασθενών, ενώ διατηρείται η ροή των πληροφοριών για δευτερεύουσες χρήσεις (Ohno-Machadoa, et al., 2004). Τεχνικές και εφαρμογές λογισμικού που παρέχουν λύσεις για την εξασφάλιση της ανωνυμίας των δεδομένων του ασθενή βρίσκονται ήδη υπό ανάπτυξη. Παρόλα αυτά, δεν υπάρχει ομοφωνία όσον αφορά το τι συνιστά ένα σύνολο ανωνυμοποιημένων δεδομένων και το πώς ο βαθμός της ανωνυμίας μπορεί να ποσοτικοποιηθεί προκειμένου να παρέχει μηχανισμούς για την τυποποίηση του προβλήματος, ή ακόμη περισσότερο το ποιες πληροφορίες θα πρέπει να θεωρούνται ευαίσθητες. Το θέμα αυτό έχει σημαντικές επιπτώσεις σε κατανεμημένα συστήματα και σε χώρους αποθήκευσης δεδομένων. Δεδομένου ότι δεν υπάρχει κοινή αντίληψη για την ανωνυμοποίηση και δεν είναι σαφές το ποια δεδομένα θεωρούνται ευαίσθητα, οι πληροφορίες που συλλέγονται από διαφορετικούς χώρους αποθήκευσης δεδομένων θα μπορούσαν ενδεχομένως να περιέχουν σύνολα δεδομένων με πληροφορίες που μπορούν να συνδεθούν με άτομα (Ohno-Machadoa, et al., 2004). Στην περίπτωση των πολλαπλών πεδίων, στην οποία οι εμπλεκόμενοι οργανισμοί δεν μοιράζονται τις ίδιες τεχνολογίες, δεν εξασφαλίζεται πλήρως η ασφαλής πρόσβαση και η αποδέσμευση πληροφοριών (Agrawal & Johnson, 2007). Για παράδειγμα, σε μεγάλο εύρος μελετών, όπου οι πληροφορίες συλλέγονται από διάφορους χώρους αποθήκευσης δεδομένων, η ύπαρξη διαφορετικών προσεγγίσεων τόσο για την αναγνώριση συνόλων ευαίσθητων δεδομένων όσο και οι τεχνολογίες που χρησιμοποιούνται για την ανωνυμοποίηση τους, θα μπορούσαν να μετατραπούν σε κινδύνους ασφάλειας που θα αποτελούσαν απειλή κατά της ιδιωτικότητας και της εμπιστευτικότητας των πληροφοριών των ασθενών.

Η χρήση ΗΑΥ περιέχει, επίσης, μια κανονιστική συνιστώσα η οποία απαιτεί ιδιαίτερη προσοχή. Η νομοθεσία και οι κανονισμοί καθορίζουν το ποιος έχει πρόσβαση στις πληροφορίες και στο πώς μπορούν να αποδεσμευθούν. Επιπλέον, αποτελεί το πλαίσιο από το οποίο καθορίζονται οι πολιτικές πρόσβασης και ασφάλειας. Οι πολιτικές για την δευτερογενή αποδέσμευση και χρήση πληροφοριών καθώς κα οι πολιτικές για την αποδέσμευση και χρήση των ΗΑΥ από τρίτα μέρη, δεν καθορίζονται μόνο από την σχετική νομοθεσία και το κανονιστικό πλαίσιο, αλλά βασίζονται και στην κουλτούρα, τις εμπειρίες και τις ηθικές αξίες των οργανισμών. Επιπλέον, η τεχνολογίες που χρησιμοποιούνται για την διατήρηση των πολιτικών και τον καθορισμό της πρόσβασης σε αποθηκευμένα δεδομένα διαφέρει από οργανισμό σε οργανισμό. Λαμβάνοντας τα παραπάνω υπόψη, είναι προφανές ότι η οποιαδήποτε ανταλλαγή δευτερογενών πληροφοριών μεταξύ των οργανισμών θα αντιμετώπιζε τελικά ασύμβατες ή αντιπαραβαλλόμενες πολιτικές (Agrawal & Johnson, 2007). Η εφαρμογή των συμφωνιών πολιτικής θα μπορούσε να προσφέρει λύσεις όσον αφορά την ύπαρξη των διαφορών μεταξύ των πολιτικών κατά την συλλογή και ανταλλαγή

των αποθηκευμένων δεδομένων. Εντούτοις, όπως έχει αναφερθεί προηγουμένως, η διαλειτουργικότητα των πολιτικών αποδέσμευσης θα εξαρτηθεί επίσης από το πόσο καλά τα πληροφοριακά συστήματα είναι σε θέση να τις ερμηνεύσουν (Blobel, 2000; Blobel, et al., 2006; Blobel & Roger-France, 2001). Η κανονικοποίηση των πολιτικών καθώς και ο κοινός ορισμός των λεξιλογίων για ερμηνεία, αποτελεί βασικό παράγοντα για την ασφαλή αποδέσμευση δευτερογενών πληροφοριών υγείας όχι μόνο για τα τοπικά περιβάλλοντα, αλλά και σε διοργανικά σενάρια.

2.7 Συμπεράσματα

Είναι κοινώς αποδεκτό ότι το ΠΣΥ αποτελεί τμήμα των κοινωνικών υποδομών για την παροχή υπηρεσιών υγείας και είναι μάλιστα το κλειδί για την βελτίωση της ποιότητας και της αποτελεσματικότητας της υγειονομικής περίθαλψης. Για την ανάπτυξη ενός ΠΣΥ χρειάζεται συνεργασία και συναίνεση από τους παρόχους υπηρεσιών υγείας, την βιομηχανία, την κυβέρνηση και την ακαδημαϊκή κοινότητα.

Σημαντική λειτουργία ενός σύγχρονου ΠΣΥ με άμεσα και ορατά οφέλη για το κοινό είναι το Ηλεκτρονικό Αρχείο Υγείας. Το ΗΑΥ περιέχει πληροφορίες που βοηθούν τους παρόχους υπηρεσιών υγείας να συνεργάζονται με σκοπό να προάγουν την υγεία του ασθενούς. Σημαντικό χαρακτηριστικό του ΗΑΥ θα πρέπει να είναι η διαλειτουργικότητα, η ικανότητα δηλαδή του συστήματος να ανταλλάσει, να συλλέγει και να διαβάζει την πληροφορία αξιοποιώντας έτσι στο μέγιστο ταχύτητα και χωρητικότητα που μας παρέχει η τεχνολογία.

Η διαλειτουργικότητα δε θα μπορούσε παρά να αποτελεί σημαντικότατη παράμετρο στο χώρο της υγείας. Η επικοινωνία και η ανταλλαγή δεδομένων μεταξύ των εμπλεκόμενων φορέων είναι μείζονος σημασίας για την ισορροπία και τη σωστή λειτουργία του όλου συστήματος. Ως εκ τούτου, θα πρέπει να βρεθεί μια φόρμουλα η οποία να ικανοποιεί την απαίτηση για αποτελεσματική ενδοεπικοινωνία μεταξύ των αλληλεπιδρώντων φορέων. Η μέχρι σήμερα επικοινωνία τους, οδηγεί σε πολλές ανθρώπινες παραλήψεις, σφάλματα, ακόμα και σε διασπάθιση δημοσίου χρήματος. Κρίνεται λοιπόν επιτακτική η ανάγκη για την δημιουργία ενός κεντρικοποιημένου και ελεγχόμενου συστήματος διαλειτουργικότητας που θα επιτρέπει την ταχύτερη, ασφαλέστερη και αποτελεσματικότερη επικοινωνία των φορέων αυτών.

Κεφάλαιο 3

Υφιστάμενο Νομοθετικό Πλαίσιο

3.1 Εισαγωγή

Ένα σημαντικό θέμα το οποίο θα πρέπει να ληφθεί υπόψη για την υλοποίηση ενός ΠΣΥ είναι η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των ασθενών. Επιπλέον, θα πρέπει να ληφθεί υπόψη η προστασία των προσωπικών δεδομένων και η εξασφάλιση ενός υψηλού επιπέδου προστασίας κατά τη διασυνοριακή διακίνησή τους.

Τα ηλεκτρονικά αρχεία υγείας περιλαμβάνουν μερικά από τα πιο ευαίσθητα δεδομένα ενός ατόμου, και επομένως αξίζουν το μεγαλύτερο βαθμό προστασίας ενάντια σε όλα τα είδη των καταχρήσεων καθιστώντας τη φύση της επεξεργασίας ευαίσθητη και απαιτώντας έτσι μεγαλύτερο και ειδικό χειρισμό στην προστασία τους. Οπόταν οποιαδήποτε επεξεργασία προσωπικών δεδομένων, θα πρέπει να ικανοποιεί τη νομοθεσία , το ιατρικό απόρρητο αλλά και τους κανόνες που υπάρχουν σχετικά με την προστασία των προσωπικών δεδομένων του ατόμου.

Το ΗΑΥ, παρόλο που είναι μια εξελισσόμενη ιδέα προσανατολιζόμενη στην παροχή βελτιωμένης και ποιοτικής φροντίδας υγείας στον ασθενή, δεν πρέπει να αφαιρεί το δικαίωμα από τον κάθε ασθενή για τη διασφάλιση της εμπιστευτικότητας και προστασίας των ευαίσθητων προσωπικών του δεδομένων, αλλά να το κατοχυρώνει. Για αυτό το λόγο, κρίνεται απαραίτητος ο καθορισμός κατάλληλου νομοθετικού πλαισίου έτσι ώστε όλες οι απαραίτητες διαδικασίες και ενέργειες που πρέπει να γίνονται να είναι συμμορφωμένες με το νόμο όπως αυτός εφαρμόζεται στο συγκεκριμένο κράτος αλλά και στην Ευρωπαϊκή Ένωση.

Τέτοιες ενέργειες συμπεριλαμβάνουν την ηλεκτρονική επεξεργασία και συλλογή των προσωπικών δεδομένων του ασθενή, καθώς και τη διακίνηση τους τόσο εντός των κρατικών συνόρων όσο και διασυνοριακά. Λόγω της ευαισθησίας των δεδομένων που λαμβάνουν μέρος στις πιο πάνω διαδικασίες, κρίνεται απαραίτητη η προστασία τους αφού πιθανή αποκάλυψή ή διαρροή τους εγκυμονεί κινδύνους τόσο στη συνεργασία του ασθενή με τον ιατρικό κόσμο όσο και με την ευρύτερη κοινωνία. Λόγω της προκατάληψης που ενδέχεται να δημιουργηθεί στον ασθενή, υπάρχει μεγάλη πιθανότητα να μην αποκαλύπτει κάποιες σημαντικές και απαραίτητες πληροφορίες που μπορούν να συμβάλουν, όχι μόνο στην ατομική του υγεία αλλά και στη δημόσια υγεία.

Η προστασία των προσωπικών δεδομένων του ατόμου και της ιδιωτικής του ζωής είναι θεμελιώδης ανθρώπινο δικαίωμα. Μέσω της νομοθεσίας παρέχονται κάποια δικαιώματα στα άτομα αλλά και κάποιες υποχρεώσεις σε αυτούς που επεξεργάζονται προσωπικά δεδομένα. Η επεξεργασία των δεδομένων πρέπει να ακολουθεί τους σχετικούς νομικούς κανονισμούς που αφορούν τόσο την προστασία των ευαίσθητων δεδομένων όσο και το ιατρικό απόρρητο.

3.2 Ιατρικό Απόρρητο

Σε όλα τα κείμενα που υπάρχουν σχετικά με την ιατρική δεοντολογία, από τα πρώτα χρόνια της εφαρμογής της ιατρικής επιστήμης μέχρι σήμερα, αναγνωρίζεται ότι το ιατρικό απόρρητο αποτελεί καθήκον του ιατρού και δικαίωμα του ασθενούς, το οποίο πρέπει να εφαρμόζεται και να λαμβάνεται σοβαρά υπόψη από παντού.

Ο κάθε ιατρός, οφείλει να τηρεί αυστηρά απόλυτη εχεμύθεια για οποιοδήποτε στοιχείο υποπίπτει στην αντίληψή του ή του αποκαλύπτει ο ασθενής ή τρίτοι, στο πλαίσιο της άσκησης των καθηκόντων του, και το οποίο αφορά τον ασθενή ή τους οικείους του. Για την αυστηρή και αποτελεσματική τήρηση του ιατρικού απορρήτου, ο ιατρός οφείλει να ασκεί την αναγκαία εποπτεία στους βοηθούς, στους συνεργάτες ή στα άλλα πρόσωπα που συμπράττουν ή συμμετέχουν ή τον στηρίζουν με οποιονδήποτε τρόπο κατά την άσκησή του. Επιπρόσθετα, να λαμβάνει κάθε μέτρο διαφύλαξης του απορρήτου ακόμη και μετά τη λήξη άσκησης του λειτουργήματος του.

Η Βρετανική Ιατρική Εταιρία αναφέρει ότι: «Ο γιατρός πρέπει να διατηρεί μυστικότητα σε όλα όσα ξέρει. Σ' αυτή τη γενική αρχή, όμως, υπάρχουν πέντε εξαιρέσεις, που αποδεσμεύουν το γιατρό από την τήρηση του απορρήτου. Αυτές είναι: όταν ο ασθενής δίνει τη συγκατάθεσή του, όταν πρόκειται για το συμφέρον του ασθενούς, όταν υπερισχύει το καθήκον του γιατρού απέναντι στην κοινωνία, για ερευνητικούς σκοπούς και αφού εγκριθεί από την αρμόδια Επιτροπή Ηθικής για την κλινική έρευνα και όταν οι πληροφορίες απαιτούνται για νομικές διαδικασίες».

Παλαιότερα κείμενα όπως είναι η Διακήρυξη της Ευρωπαϊκής Ένωσης των Γενικών Ιατρών για το Ιατρικό Απόρρητο και η απόφαση της Παγκόσμιας ιατρικής ένωσης για τη χρησιμοποίηση των ηλεκτρονικών υπολογιστών στην ιατρική, αποτελούν κείμενα τα οποία ίσως αποθαρρύνουν τους ιατρούς να χρησιμοποιήσουν τον ηλεκτρονικό φάκελο ή αν το χρησιμοποιήσουν, να είναι πολύ προσεκτικοί και αυστηροί.

Καινούργιες ανακοινώσεις του Ευρωπαϊκού Κοινοβουλίου, όπως είναι το πρόγραμμα δράσης «ηλ-υγεία», τονίζει πως οι τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ - ICT) μπορούν να χρησιμοποιηθούν για την παροχή ποιοτικότερων υπηρεσιών ιατροφαρμακευτικής περίθαλψης

σε ολόκληρη την Κοινότητα. Κυρίαρχος στόχος της δράσης, είναι η δημιουργία «ευρωπαϊκού χώρου ηλεκτρονικής-υγείας» και καταγραφή πρακτικών μέτρων που θα εφαρμοστούν σε διάφορους τομείς της ηλεκτρονικής υγείας όπως στους ηλεκτρονικούς φακέλους και στην ταυτοποίηση των ασθενών και στις κάρτες υγείας. Ο απώτερος στόχος του προγράμματος είναι να ενταχθεί η ηλ-υγεία στις συνήθειες των επαγγελματιών της υγείας, των ασθενών και των πολιτών.

Το ΗΑΥ, θεωρείται από πολλούς, ότι μπορεί να καταπατήσει το ιατρικό απόρρητο. Παρόλο που η δημιουργία και η χρήση του είναι πολύ χρήσιμη σε πολλούς τομείς, εφόσον αποθηκεύονται πολλές και χρήσιμες πληροφορίες με άμεση πρόσβαση από τον ιατρό και δυνατότητα αποδοτικής επεξεργασίας τους, μπορεί να αποτελέσει κίνδυνο όσον αφορά την εμπιστευτικότητα και την ιδιωτικότητα του ασθενή καθώς και καταπάτηση του ιατρικού απορρήτου. Για το λόγο αυτό, είναι απαραίτητη η ύπαρξη νομοθεσίας, ώστε η υλοποίηση και η εφαρμογή του να γίνει εφικτή και αποτελεσματική.

3.3 Προκλήσεις Νομοθεσίας στον τομέα της Υγείας

Οι συμμετέχοντες στον χώρου του ηλεκτρονικού αρχείου υγείας του ασθενή, μπορούν να ταξινομηθούν σε τέσσερις ομάδες :

- Πολίτες και ασθενείς
- Νοσοκομειακοί γιατροί και οι παροχείς υπηρεσιών υγείας
- Κυβερνήσεις και άτομα για οργάνωση στρατηγικών και
- Προμηθευτές υπηρεσιών και ιατρικού εξοπλισμού

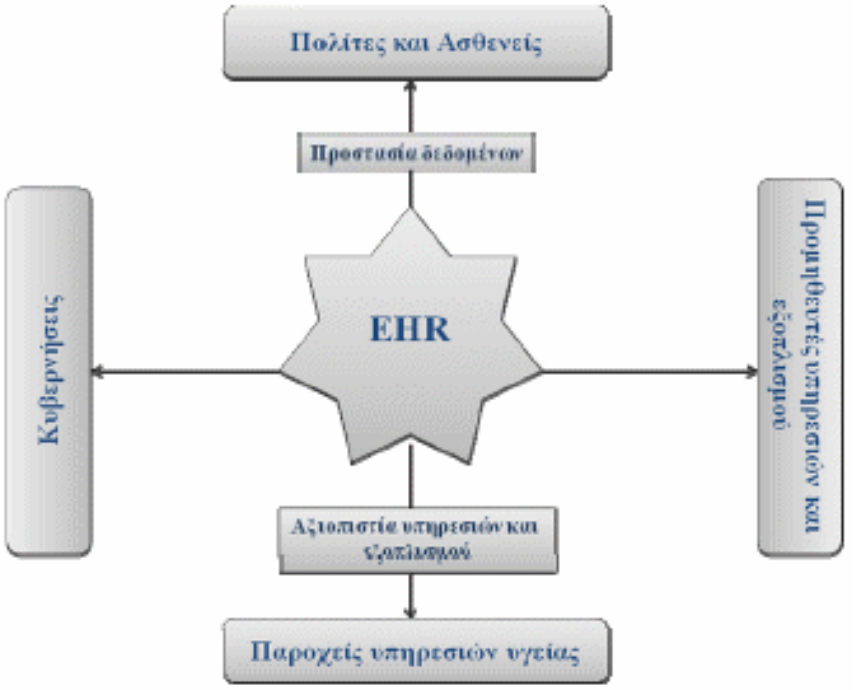
Και οι τέσσερις ομάδες έχουν ιδιαίτερα σημαντικούς αλλά όχι πάντα ίσους ρόλους στην υγειονομική περίθαλψη. Οι συμμετέχοντες στον χώρο της υγείας, συνήθως έχουν περιορισμένη αντίληψη ως προς τις ανάγκες του κάθε ενός ξεχωριστά. Επιπρόσθετα, οι συμμετέχοντες έχουν περιορισμένη αναγνώριση των νομικών τους υποχρεώσεων και έτσι συνήθως θα είναι πολύ δύσκολο να εκμεταλλευτούν το γεγονός ότι μέσω του ΗΑΥ του ασθενή μπορούν να επικοινωνήσουν άμεσα.

Συνήθως οι εντάσεις προκύπτουν μεταξύ των νοσοκομειακών ιατρών και των ασθενών για θέματα εμπιστευτικότητας και μυστικότητας ή μεταξύ κυβερνήσεων μεταξύ προμηθευτών υπηρεσιών και ιατρικού εξοπλισμού όσον αφορά τον ανταγωνισμό στην αγορά υγειονομικής περίθαλψης. Η ένταση είναι κυρίως διακριτή στον ηλεκτρονικό φάκελο , ο οποίος αντιμετωπίζεται σαν μια τεχνολογική λύση παρά ως ένα βασικό εργαλείο των υπηρεσιών υγείας που έχει μεγάλη συνεισφορά σε κοινές αρχές ισότιμης, αποδοτικής και ασφαλούς περίθαλψης.

Για να μπορέσουν οι συμμετέχοντες να κατανοήσουν τον ηλεκτρονικό φάκελο ασθενή και τη μεγαλύτερη χρήση του, θα πρέπει να κατανοήσουν όχι μόνο το τεχνικό περιεχόμενο, αλλά να αναπτύξουν και μια βαθύτερη κατανόηση των νομικών, ηθικών και κοινωνικών ζητημάτων που προέρχονται από τη χρήση του ηλεκτρονικού φακέλου.

Δεδομένου ότι το ΗΑΥ του ασθενή εξαρτάται από τη συλλογή και τη διανομή των δεδομένων των ασθενών, είναι σημαντικό να εξεταστεί ο βαθμός στον οποίο οι νόμοι που υπάρχουν για την προστασία δεδομένων και της μυστικότητας συγκρούονται με τη γενική ιδέα του ΗΑΥ του ασθενή.

Επιπλέον, δεδομένου ότι το ΗΑΥ θα χρησιμοποιηθεί για τη διευκόλυνση της συνεργασίας μεταξύ των διαφόρων παρόχων υπηρεσιών υγείας, είναι σημαντικό να εξεταστεί μέχρι ποιό σημείο οι παρόντες κανονισμοί και νόμοι για την ευθύνη των προϊόντων και των υπηρεσιών, καλύπτουν τη χρήση εργαλείων βελτίωσης της παροχής υπηρεσιών υγείας, όπως είναι το ΗΑΥ του ασθενή.



Σχήμα 3.1 *Συμμετέχοντες στον χώρο του ΗΑΥ*

Η πρόκληση είναι σαφής: ένα ΠΣΥ, μπορεί να χρησιμοποιηθεί στο μέγιστο των δυνατοτήτων του, όταν το όλοι οι συμμετέχοντες στον χώρο της υγείας μπορούν να έχουν πρόσβαση στα δεδομένα όταν τα χρειάζονται. Συγχρόνως, πρέπει να διασφαλιστεί ότι οι συμμετέχοντες θα έχουν στη διάθεσή τους μόνο τα δεδομένα που χρειάζονται για την εκπλήρωση των στόχων τους και όχι περισσότερα. Ακόμη, θα πρέπει να υπάρχουν οι μηχανισμοί οι οποίοι θα διασφαλίζουν ότι τα στοιχεία δεν θα μπορούν να είναι προσπελάσιμα από μη-εξουσιοδοτημένα πρόσωπα ή οργανώσεις.

Όλες οι χώρες που έχουν λάβει την απόφαση δημιουργίας ενός συστήματος ΗΑΥ, πριν την εκπόνηση του σχεδιασμού, αναλώθηκαν σε μελέτες των διάφορων Ευρωπαϊκών οδηγιών, κανονισμών, εισηγήσεων και άλλων διεθνών νομοθεσιών που θεσπίστηκαν στα πλαίσια της προσπάθειάς τους να δημιουργήσουν ανάλογα συστήματα . Αυτό έχει γίνει για να διαπιστωθεί εάν η υπάρχουσα νομοθεσία συγκρούεται με τη γενική ιδέα του ΗΑΥ του ασθενή και κατά πόσο μπορεί να ανταπεξέλθει στην εμφάνιση των νέων αναγκών που προκύπτουν.

3.4 Νομοθετικό Πλαίσιο Προστασίας Προσωπικών Δεδομένων στην Ευρωπαϊκή Ένωση

Η εφαρμογή ενός ΠΣΥ, από τη φύση του, θα περιλαμβάνει την επεξεργασία πληροφοριών σχετικά με έναν ασθενή. Το ΗΑΥ διευκολύνει τη συνεργασία και την επικοινωνία μεταξύ ενός ευρύτερου πεδίου από συμμετέχοντες όπως είναι οι επαγγελματίες υγείας, οι ασθενείς, οι ασφαλιστικές εταιρείες, οι προμηθευτές ιατρικών τεχνολογιών πληροφορικής, φαρμακευτικές εταιρείες, ρυθμιστικές αρχές, ακαδημαϊκούς και άλλους ερευνητές. Οι συμμετέχοντες, στα πλαίσια της παροχής βελτιωμένης ιατρικής περίθαλψης, θα ανταλλάζουν πληροφορίες τόσο σε τοπικό όσο και σε ευρωπαϊκό και διεθνές επίπεδο. Αυτές οι πληροφορίες, σύμφωνα με τη νομοθεσία, εμπίπτουν στην κατηγορία των προσωπικών δεδομένων που υπόκεινται στη νομοθεσία που αφορά την προστασία δεδομένων.

Όλα τα άτομα και όλοι οι ασθενείς έχουν το δικαίωμα στην ιδιωτική ζωή. Συνεπώς αναμένεται από όλους του φορείς παροχής ιατρικής περίθαλψης αλλά και κάθε άλλο συμμετέχοντα σε ένα ΠΣΥ, να τηρούν την προστασία των προσωπικών πληροφοριών και το απόρρητο. Το ίδιο θα πρέπει να ισχύει και για τα ΠΣΥ τα οποία μέσα από κατάλληλους μηχανισμούς θα πρέπει να κατοχυρώνουν το δικαίωμα της ιδιωτικότητας και της εμπιστευτικότητας.

Οι εξελίξεις σε μια ελεύθερη, απαλλαγμένη από σύνορα κοινωνία της πληροφορίας, αύξησε τις διακρατικές ροές των προσωπικών δεδομένων μεταξύ των κρατών μελών της ΕΕ και όχι μόνο. Προκειμένου να αφαιρεθούν πιθανά εμπόδια από την ύπαρξη τέτοιων ροών και για να εξασφαλιστεί ένα υψηλό επίπεδο προστασίας εντός της ΕΕ, η Ευρωπαϊκή Κοινότητα έχει θεσπίσει νομοθεσία που αφορά την προστασία των προσωπικών δεδομένων.

Η Ευρωπαϊκή Επιτροπή (Commission) συμμετέχει σε διαλόγους και με χώρες που βρίσκονται εκτός της Ευρωπαϊκής Ένωσης προκειμένου να διασφαλιστεί ένα υψηλό επίπεδο της προστασίας κατά τη διακίνηση των προσωπικών στοιχείων σε εκείνες τις χώρες. Ενθαρρύνει μελέτες για την ανάπτυξη του επιπέδου της προστασίας δεδομένων σε ευρωπαϊκό και διεθνές επίπεδο.

Στην Ευρώπη, η προστασία των δεδομένων παρέχεται μέσα από νομικούς κανόνες οι οποίοι απορρέουν από διάφορες νομικές πηγές (όπως είναι οδηγίες, προτάσεις κλπ), ο σημαντικότερος των οποίων είναι η οδηγία για τη προστασία δεδομένων (οδηγία 95/46/ΕΚ), η οποία τώρα έχει μετατραπεί σε εθνική νομοθεσία προστασίας δεδομένων σε ολόκληρη την ΕΕ.

Η λειτουργία των ΠΣΥ πρέπει να τηρεί τις αρχές προστασίας των προσωπικών δεδομένων που προβλέπονται στις ευρωπαϊκές οδηγίες. Η τήρηση αυτών των αρχών, ενισχύει όλους τους συμμετέχοντες φορείς του χώρου της υγείας και τα ιδρύματα παρέχοντάς του τα απαραίτητα κίνητρα που θα διασφαλίσουν την καλύτερη λειτουργία των συστημάτων αυτών.

Το θεμελιώδες δικαίωμα της προστασίας των δεδομένων προσωπικού χαρακτήρα απορρέει κατά κύριο λόγο από το άρθρο 8 της ευρωπαϊκής σύμβασης για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών και του άρθρου 8 του Χάρτη Θεμελιωδών Δικαιωμάτων. Έχουν θεσπιστεί πιο σαφείς κανόνες και έχουν δοθεί πιο ακριβής κατευθυντήριες γραμμές σε ένα σύνολο οδηγιών που έχουν εκδοθεί στα πλαίσια της Ευρωπαϊκής Ένωσης με πιο χαρακτηριστική την οδηγία για την προστασία των δεδομένων προσωπικού χαρακτήρα 95/46/ΕΚ και στην οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Ακριβέστεροι κανόνες καθορίστηκαν και στις εθνικές νομοθεσίες των κρατών μελών που έχουν την υποχρέωση να μεταφέρουν τις οδηγίες αυτές εναρμονίζοντάς τις σε εθνικό επίπεδο.

Οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των συστημάτων ΗΑΥ, θα πρέπει να υπακούει και στους κανόνες που θεσπίστηκαν στη σύμβαση του Συμβουλίου της Ευρώπης για την προστασία των ατόμων κατά την αυτόματη επεξεργασία των προσωπικών δεδομένων από υπολογιστή καθώς και στο πρόσθετο πρωτόκολλο στη σύμβαση 108 για τις εποπτικές αρχές και τη διασυνοριακή διακίνηση των δεδομένων.

Στο πλαίσιο της εφαρμογής του ΗΑΥ, εμπίπτει και η σύσταση του Συμβουλίου της Ευρώπης R(97) 5 η οποία αναφέρεται στην προστασία των ιατρικών δεδομένων. Πιο κάτω, γίνεται αναφορά σε ένα σύνολο συστάσεων η οποίες θα διαδραματίσουν ρόλο στην ηλεκτρονική διάθεση των ιατρικών αρχείων των ασθενών.

3.4.1 Συστάσεις και Οδηγίες της Ευρωπαϊκής Ένωσης για την Προστασία Προσωπικών Δεδομένων

Σύσταση για την προστασία των ατόμων όσον αφορά την αυτοματοποιημένη επεξεργασία των προσωπικών δεδομένων CETS No.: 108: Η σύσταση αυτή, η οποία υπογράφηκε ήδη από το 1981, αποτελεί το πρώτο διεθνές όργανο, για την προστασία του ατόμου από τη συλλογή και αυτοματοποιημένη επεξεργασία των προσωπικών του δεδομένων και προσπαθεί να ρυθμίσει τη

διασυνοριακή διακίνηση των προσωπικών δεδομένων όπου η αντίστοιχη νομοθεσία δεν παρέχει ισοδύναμη προστασία.

Τα δεδομένα τα οποία συλλέγονται για την αυτοματοποιημένη επεξεργασία, πρέπει να αναφέρονται στον συγκεκριμένο σκοπό της επεξεργασίας και δεν πρέπει να χρησιμοποιούνται για κανένα άλλον σκοπό. Τα δεδομένα πρέπει να είναι επαρκή, ακριβή για τον σκοπό της επεξεργασίας και να αποθηκεύονται μόνο για το συγκεκριμένο χρονικό διάστημα για το οποίο διαρκεί η επεξεργασία. Η Συνθήκη διαφυλάσσει το δικαίωμα του κάθε ατόμου να γνωρίζει ποιες πληροφορίες αποθηκεύονται για το άτομό του και σε περίπτωση σφάλματος να μπορούν να διορθωθούν.

Η Συνθήκη επιβάλλει επίσης μερικούς περιορισμούς στις διασυνοριακές ροές των προσωπικών στοιχείων στα κράτη όπου ο νομικός κανονισμός δεν παρέχει την ισοδύναμη προστασία. Για την αντιμετώπιση αυτών των προβλημάτων, διαμορφώθηκε ένα Model Contract το οποίο χρησιμοποιείται σε μεγάλο βαθμό από ιδιώτες.

Η σύμβαση αυτή όμως δεν συμπεριλαμβάνει την προστασία της αυτοματοποιημένης επεξεργασίας ευαίσθητων δεδομένων στα οποία συγκαταλέγονται και τα ιατρικά δεδομένα και έτσι δημιουργείται η ανάγκη εισαγωγής καινούργιων νομοθετικών μέτρων.

Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών: Στην Ευρωπαϊκή Ένωση, η οδηγία 95/46/ΕΚ αποτελεί την πιο σημαντική οδηγία που σχετίζεται με την προστασία των προσωπικών δεδομένων. Θεσπίζει ένα κανονιστικό πλαίσιο με σκοπό την εγκαθίδρυση μιας ισορροπίας που θα διασφαλίζει ένα υψηλό επίπεδο προστασίας της ιδιωτικής ζωής των προσώπων και ελεύθερη κυκλοφορία των προσωπικών δεδομένων στο χώρο της Ευρωπαϊκής Ένωσης (ΕΕ). Η οδηγία ορίζει τα όρια για τη συλλογή και τη χρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα και ζητά τη δημιουργία, σε κάθε κράτος μέλος, ενός ανεξάρτητου εθνικού οργανισμού με αρμοδιότητα την προστασία αυτών των δεδομένων.

- *Πεδίο Εφαρμογής*

Η οδηγία αυτή ισχύει για δεδομένα τα οποία επεξεργάζονται με αυτοματοποιημένες διαδικασίες καθώς και για δεδομένα τα οποία επεξεργάζονται με μη αυτοματοποιημένες διαδικασίες που περιλαμβάνονται ή θα περιληφθούν σε αρχείο.

Τα δεδομένα που καλύπτει αυτή η οδηγία αφορούν δεδομένα τα οποία μπορούν να χρησιμοποιηθούν για τον προσδιορισμό ενός συγκεκριμένου προσώπου και δεδομένα τα οποία πρόκειται να επεξεργαστούν από ένα πρόσωπο. Για παράδειγμα, τα εργαστηριακά αποτελέσματα ενός δείγματος αίματος θα καλύπτονται από αυτή τη νομοθεσία εάν είναι δυνατό

με κάποιο τρόπο να αναγνωριστεί ο ασθενής από τον οποίο έχει παρθεί το δείγμα. Αυτή η οδηγία εφαρμόζεται ακόμα και στην περίπτωση που τα εργαστηριακά αποτελέσματα αποθηκεύονται με κωδικοποιημένα αναγνωριστικά, όπως είναι ο αναγνωριστικός αριθμός ενός ασθενή.

Η βασική ιδέα είναι ότι εάν υπάρχει ένα κομμάτι πληροφορίας το οποίο μπορεί να συνδεθεί με ένα πρόσωπο, είτε μέσω της χρήσης απλών τεχνικών είτε με τη χρήση ενός τρίτου προσώπου, τότε τα δεδομένα αυτά θεωρούνται ως δεδομένα τα οποία μπορούν να χαρακτηρίσουν οποιοδήποτε άτομο και κατά συνέπεια εμπίπτουν στο επίπεδο εφαρμογής της οδηγίας.

Εάν η πληροφορία αναφέρεται σε ένα σύνολο ατόμων ή εάν είναι τόσο ολοκληρωμένη ή μοναδική έτσι ώστε να βρίσκει εφαρμογή σε μια πολύ μικρή ομάδα ατόμων όπως για παράδειγμα, ιδιότητα (profile) ασθένειας, ηλικία, ταχυδρομικός κώδικας, τότε τα δεδομένα μπορούν να κατηγοριοποιηθούν στα πλαίσια της οδηγίας αυτής, έστω και αν δεν αποτελούν πραγματικά αναγνωριστικά δεδομένα.

Η οδηγία δεν ισχύει για την επεξεργασία δεδομένων η οποία γίνεται από κάποιο φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων ή στην περίπτωση που η επεξεργασία γίνεται για δραστηριότητες εκτός του κοινοτικού δικαίου όπως είναι η δημόσια ασφάλεια.

- *Ποιότητα των δεδομένων*

Τα προσωπικά δεδομένα θα πρέπει να συλλέγονται για σαφείς , καθορισμένους και προπαντός νόμιμους σκοπούς. Πρέπει να πληρούν συγκεκριμένα επίπεδα ποιότητας και να συμμορφώνονται με διάφορους κανόνες που αφορούν τη συλλογή και επεξεργασία των δεδομένων. Οι κανόνες οι οποίοι πρέπει να πληρούνται, στο πλαίσιο της εφαρμογής των ΠΣΥ, είναι οι πιο κάτω:

- Τα δεδομένα θα πρέπει να είναι ενημερωμένα και να διέπονται από ακρίβεια.
- Η επεξεργασία των δεδομένων θα πρέπει να διέπεται από το νόμο.
- Η συλλογή και η επεξεργασία των δεδομένων πρέπει να γίνεται για καθορισμένους και σαφείς σκοπούς και τυχόν μετέπειτα επεξεργασία τους για στατιστικούς ή ερευνητικούς σκοπούς να είναι στα πλαίσια του νόμου εφόσον προβλέπονται οι κατάλληλες εγγυήσεις από τα κράτη μέλη.
- Τα δεδομένα που συλλέγονται δεν πρέπει να είναι περισσότερα από όσα χρειάζονται για τους σκοπούς της επεξεργασίας του ΗΑΥ του ασθενή.
- Η επεξεργασία των δεδομένων θα πρέπει να χαρακτηρίζεται από διαφάνεια.
- Τα δεδομένα που συλλέγονται θα πρέπει να συνάδουν με το θέμα της επεξεργασίας.

- Η μορφή στην οποία διατηρούνται θα πρέπει να επιτρέπει τον προσδιορισμό της ταυτότητας των ατόμων που αφορούν τα δεδομένα. Αυτό πρέπει να γίνεται μόνο κατά την απαραίτητη περίοδο που τίθεται για την διάρκεια της επεξεργασίας των δεδομένων.

Συνεπώς, ένας ιατρός ο οποίος μπορεί να μοιράζεται με κάποιο άλλο ιατρό δεδομένα ασθενών για σκοπούς διάγνωσης και θεραπείας του ατόμου, τα οποία δύναται να αναγνωριστούν, τότε μπορεί να μοιράζεται τις ίδιες πληροφορίες και με κάποιο άλλο επαγγελματία της υγείας για σκοπούς ιατρικής έρευνας εάν ο σκοπός της έρευνας καθορίστηκε ως μια από τις τελικές χρήσεις των δεδομένων. Δηλαδή, εάν ο ασθενής έχει δώσει τη συγκατάθεση του για τη χρήση των δεδομένων του για τον συγκεκριμένο σκοπό ή εάν λαμβάνονται τα κατάλληλα μέτρα προστασίας για την επεξεργασία των δεδομένων για ερευνητικούς σκοπούς.

Εάν τα δεδομένα του ασθενή γίνουν ανώνυμα, τότε δεν υπάρχει κανένα πρόβλημα για τη μεταφορά των δεδομένων αυτών σε ένα τρίτο οργανισμό ή άτομο για επιστημονικούς σκοπούς όπως η ιατρική έρευνα.

- *Νόμιμη Επεξεργασία δεδομένων*

Η επεξεργασία των προσωπικών δεδομένων ενός ατόμου θα πρέπει να γίνεται εφόσον το άτομο έχει δώσει την πλήρη συγκατάθεσή του ή αν η επεξεργασία είναι απαραίτητη για τους πιο κάτω σκοπούς:

- την εκτέλεση σύμβασης της οποίας το πρόσωπο το οποίο αφορούν τα δεδομένα προς επεξεργασία λαμβάνει μέρος,
- την τήρηση νομικής υποχρέωσης στην οποία υπόκειται το άτομο που επεξεργάζεται τα δεδομένα,
- τη διαφύλαξη ζωτικού συμφέροντος του προσώπου,
- την εκτέλεση δημόσιου συμφέροντος,
- την υλοποίηση του θεμιτού συμφέροντος που επιδιώκεται από το άτομο που επεξεργάζεται τα δεδομένα.

- *Κατηγορία Ειδικών δεδομένων*

Σύμφωνα με την οδηγία, η επεξεργασία των ευαίσθητων προσωπικών δεδομένων, συμπεριλαμβανομένων και των δεδομένων σχετικά με την υγεία, απαγορεύεται. Ο σκοπός που απαγορεύεται η επεξεργασία είναι για τη διασφάλιση των θεμελιωδών δικαιωμάτων του ατόμου του οποίου τα στοιχεία έχουν χρησιμοποιηθεί για επεξεργασία. Η επεξεργασία επιτρέπεται μόνο για συγκεκριμένους σκοπούς και κάτω από την ύπαρξη συγκεκριμένων κανόνων. Η επεξεργασία τέτοιων δεδομένων μπορεί να γίνει εφικτή εφόσον:

- Όταν το άτομο στο οποίο αναφέρονται τα δεδομένα έχει δώσει την συγκατάθεσή του για επεξεργασία.
- Όταν η επεξεργασία είναι απαραίτητη στα πλαίσια της εκτέλεσης των επαγγελματικών υποχρεώσεων του υπεύθυνου επεξεργασίας των δεδομένων σε βαθμό πάντα που επιτρέπει η νομοθεσία του κράτους.
- Όταν η επεξεργασία των δεδομένων γίνεται από επαγγελματίες υγείας για σκοπούς διεκπεραίωσης ιατρικής διάγνωσης ή παροχής ιατροφαρμακευτικής αγωγής και περίθαλψης του ασθενή σε βαθμό που επιτρέπεται από τη νομοθεσία του κράτους και το επαγγελματικό ιατρικό απόρρητο.
- Όταν η επεξεργασία γίνεται για το συμφέρον καθοριστικής σημασίας του ατόμου ή κάποιου τρίτου ατόμου, σε περιπτώσεις που το άτομο είναι αδύνατο να δώσει τη συγκατάθεσή του.
- Όταν η επεξεργασία πραγματοποιείται από κάποιους μη κερδοσκοπικούς φορείς ή ιδρύματα οι οποίοι εξασφαλίζουν ότι η επεξεργασία αφορά τα μέλη τα οποία ανήκουν στο ίδρυμα ή φορέα.
- Όταν τα δεδομένα αποτελούν τεκμήρια ενώπιων δικαστηρίου και τα οποία δημοσιοποιούνται για νομικούς σκοπούς.
- Σε περίπτωση που τα δεδομένα τα οποία χρησιμοποιούνται για επεξεργασία δημοσιοποιούνται από το ίδιο το πρόσωπο στο οποίο αναφέρονται.

Κατά συνέπεια, όλα τα δεδομένα τα οποία εμπεριέχονται στο ΗΑΥ του ασθενή, θα πρέπει να θεωρούνται ως ευαίσθητα δεδομένα προσωπικού χαρακτήρα. Για το λόγο αυτό θα πρέπει να βρίσκονται υπό την αιγίδα των κανόνων της κατηγορίας των ειδικών δεδομένων και όχι σε όλους τους γενικούς κανόνες για την προστασία των προσωπικών δεδομένων.

Επιπλέον, λόγω της ευαίσθητης φύσης των δεδομένων στον ιατρικό φάκελο, θα πρέπει να περιλαμβάνονται μόνο εκείνα τα δεδομένα που συνδέονται στενά με την περιγραφή της κατάστασης της υγείας του ασθενή. Στα στοιχεία αυτά ανήκουν ακόμα και μερικά στοιχεία τα οποία δεν έχουν άμεση σχέση με την υγεία του ασθενή, όπως για παράδειγμα διοικητικά στοιχεία τέτοια όπως η ημερομηνία εισαγωγής του σε ένα νοσοκομείο. Περιλαμβάνονται όμως στον ιατρικό του φάκελο γιατί εμπίπτουν στο πλαίσιο θεραπείας του.

Η επεξεργασία των ευαίσθητων δεδομένων του ασθενή μπορεί να γίνει εφικτή εάν είναι απαραίτητη η διασφάλιση του ζωτικού του συμφέροντος. Στα πλαίσια μιας κατάστασης στην οποία ο ασθενής δεν είναι σε θέση να εκφράσει τη συγκατάθεσή του, και η πρόσβαση στο ιατρικό του ιστορικό είναι ζωτικής σημασίας για την περαιτέρω πορεία της θεραπείας του, το ιατρικό προσωπικό μπορεί να αποκτήσει πρόσβαση στα ιατρικά δεδομένα.

Για παράδειγμα, ας υποθέσουμε κάποιο πρόσωπο το οποίο έχει υποστεί κάποιο ατύχημα και δεν είναι σε θέση να δώσει τη συγκατάθεσή του ώστε οι ιατροί που ανέλαβαν τη θεραπεία του να έχουν πρόσβαση στις πληροφορίες που αφορούν αλλεργίες. Με βάση την οδηγία, οι επαγγελματίες του χώρου της υγείας επιτρέπεται να έχουν πρόσβαση στα ιατρικά του δεδομένα ώστε να διαπιστώσουν τυχόν αλλεργίες του ασθενή σε φάρμακα, γεγονός καθοριστικό για τη διεξαγωγή της θεραπείας του.

- *Συγκατάθεση του ασθενή*

Για να γίνει εφικτή η επεξεργασία των προσωπικών δεδομένων του ασθενή, ο ασθενής θα πρέπει να δώσει τη συγκατάθεσή του. Η συγκατάθεση του ασθενή, με βάση την οδηγία θα πρέπει να είναι «ελεύθερη», «ρητή» και «εν πλήρη επιγνώσει».

Με τον όρο «ελεύθερη» συγκατάθεση, νοείται ότι ο ασθενής ο οποίος δεν αντιμετωπίζει οποιοδήποτε νοητικό πρόβλημα, δίνει τη συγκατάθεση του με τη θέλησή του, χωρίς να βρίσκεται κάτω από οποιοδήποτε είδος εξαναγκασμού όπως για παράδειγμα κάτω από οικονομική ή ψυχολογική πίεση. Όταν ένας επαγγελματίας υγείας επεξεργάζεται δεδομένα στο πλαίσιο ενός συστήματος ηλεκτρονικού φακέλου ασθενή, δεν δικαιολογείται να νομιμοποιεί με κακοπροαίρετους σκοπούς την επεξεργασία παραπλανώντας τον ασθενή να δώσει τη συγκατάθεσή του.

Με τον όρο «ρητή» συγκατάθεση, νοείται ότι η συγκατάθεση του ασθενή θα πρέπει να συνοδεύεται από τους άμεσους σκοπούς της επεξεργασίας των δεδομένων. Συνεπώς, εάν ο ασθενής δώσει τη συγκατάθεση του για την επεξεργασία των προσωπικών του δεδομένων από έναν προσωπικό του ιατρό, τότε η μεταβίβαση τους σε άλλους επαγγελματίες και κατόπιν η επεξεργασία τους, δεν καλύπτεται από τη ρητή συγκατάθεση του ασθενή.

Με τον όρο «εν πλήρη επιγνώσει», νοείται ότι ο ασθενής έχει επίγνωση των επακόλουθων πράξεων του. Και πάλι, ο ασθενής θα πρέπει να ενημερωθεί με σαφή και κατανοητό τρόπο να ενημερωθεί για τους σκοπούς επεξεργασίας, το επίπεδο πρόσβασης στα δεδομένα που θα έχουν οι αποδέκτες των δεδομένων.

Κάποιες φορές, η εξασφάλιση της συγκατάθεσης του ασθενή είναι εξαιρετικά δύσκολη, ειδικότερα όταν δεν υπάρχει άμεση επικοινωνία μεταξύ του υπεύθυνου της επεξεργασίας και των ατόμων στων οποίων ανήκουν τα δεδομένα. Παρόλα αυτά, ο υπεύθυνος της επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι πέτυχε τη ρητή, ελεύθερη και την εν πλήρη επιγνώσει συγκατάθεση των ασθενών.

- *Ενημέρωση του προσώπου του οποίου τα δεδομένα θα τύχουν επεξεργασίας*

Οι υπεύθυνοι επεξεργασίας που επεξεργάζονται πληροφορίες στο πλαίσιο των ΠΣΥ, πρέπει να παρέχουν στα πρόσωπα από τα οποία συλλέγοντα δεδομένα ενημέρωση σχετικά με:

- την ταυτότητά του και αυτόν που εκπροσωπεί (εάν υπάρχει)
- τον σκοπό που γίνεται η επεξεργασία
- πληροφορίες που αφορούν τους αποδέκτες των δεδομένων
- Κατά πόσο η παροχή των προσωπικών δεδομένων είναι υποχρεωτική ή εθελοντική

➢ *Δικαίωμα πρόσβασης του προσώπου στου οποίου αναφέρονται τα δεδομένα*

Η οδηγία αυτή, δεν δημιουργεί μόνο υποχρεώσεις στα άτομα τα οποία συλλέγουν τα δεδομένα, αλλά εξασφαλίζει δικαιώματα στα άτομα των οποίων τα δεδομένα πρόκειται να επεξεργαστούν, όπως είναι οι ασθενείς.

Κάθε άτομο του οποίου τα προσωπικά δεδομένα, συμπεριλαμβανομένων και των δεδομένων υγείας, τυχαίνουν επεξεργασίας, έχει το δικαίωμα να διορθώσει, να διαγράψει ή και να απαγορεύσει την πρόσβαση σε δεδομένα των οποίων η επεξεργασία δεν συμφωνεί με την τρέχουσα επεξεργασία. Επιπλέον, μπορεί να απαγορεύσει την γνωστοποίηση των τροποποιήσεων αυτών προς τρίτους προς τους οποίους τα δεδομένα αυτά έχουν διαβιβασθεί. Επίσης έχει το δικαίωμα να διαβεβαιωθεί αν τα δεδομένα που το αφορούν αποτελούν ή δεν αποτελούν αντικείμενο επεξεργασίας καθώς και να γνωστοποιηθούν σε αυτόν τα δεδομένα που θα αποτελέσουν το αντικείμενο επεξεργασίας.

Το δικαίωμα πρόσβασης και η ενημέρωση του ατόμου σχετικά με την επεξεργασία των προσωπικών του δεδομένων μπορεί να μην πραγματοποιηθεί σε περιπτώσεις που τα θεμελιώδη δικαιώματα και ελευθερίες του συγκεκριμένου ατόμου ή άλλων ατόμων πρέπει να προστατευθούν. Επιπλέον, σε περιπτώσεις όπου η επεξεργασία των δεδομένων σχετίζεται με την ασφάλεια του κράτους, τη δημόσια ασφάλεια, την άμυνα και σε περιπτώσεις διερεύνησης και πρόληψης καθώς και περιπτώσεις παραβάσεων του ποινικού νόμου κλπ.

Πάνω σε αυτή τη βάση, οι περισσότερες ευρωπαϊκές χώρες έχουν εισάγει νομοθεσίες που επιτρέπουν την πρόσβαση των ασθενών στα προσωπικά τους ιατρικά αρχεία.

➢ *Μεταφορά δεδομένων σε τρίτες χώρες*

Οι μεταβιβάσεις δεδομένων προσωπικού χαρακτήρα από ένα κράτος μέλος σε τρίτη χώρα, επιτρέπονται υπό την προϋπόθεση ότι η εν λόγω τρίτη χώρα διαθέτει το κατάλληλο επίπεδο προστασίας. Αντίθετα, οι εν λόγω μεταβιβάσεις δεν μπορούν να πραγματοποιηθούν προς τρίτες χώρες οι οποίες δεν διαθέτουν το κατάλληλο επίπεδο προστασίας. Μπορούν να γίνουν κάποιες εξαιρέσεις σε περιπτώσεις όπου ο υπεύθυνος επεξεργασίας μπορεί να εγγυηθεί ότι ο παραλήπτης των δεδομένων θα μπορεί να εναρμονιστεί με τους κανόνες που αφορούν την προστασία των δεδομένων.

- *Αρχή ελέγχου και ομάδα για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα*

Κάθε κράτος πρέπει να δημιουργεί μια αρχή ελέγχου η οποία θα επιφορτίζεται με τον έλεγχο του επιπέδου προστασίας των δεδομένων σε ένα κράτος μέλος. Θα είναι υπεύθυνη να δίνει συμβουλές στην κυβέρνηση για διαχειριστικά μέτρα και κανονισμούς. Επιπλέον, θα θέτει σε εφαρμογή νομικές διαδικασίες σε περιπτώσεις που κανονισμοί σχετικά με την προστασία των δικαιωμάτων έχουν παραβιαστεί(άρθρο 28). Τα άτομα μπορούν να εκθέτουν τα παράπονά τους σχετικά με παραβιάσεις στην αρμόδια αρχή ελέγχου, είτε στο δικαστήριο.

- *Υλοποίηση στα κράτη μέλη*

Η συγκεκριμένη οδηγία έχει υιοθετηθεί από όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης και έχουν συνταχθεί οι ανάλογοι εθνικοί νόμοι.

Για να γίνει σαφές το πλαίσιο εφαρμογής της συγκεκριμένης οδηγίας στα πλαίσια του ΗΑΥ του ασθενή, δίνεται ένα παράδειγμα για το πως οι κανόνες που αφορούν την προστασία των δεδομένων, εφαρμόζονται στην πράξη.

- *Παράδειγμα 1 – Μεταφορά δεδομένων υγείας*

Ο ασθενή Χ επισκέπτεται ένα ίδρυμα παροχής ιατρικής περίθαλψης στη χώρα του για να πραγματοποιήσει ιατρικές εξετάσεις για τον εντοπισμό του προβλήματος που του προκαλεί πόνο στην κοιλιακή χώρα. Ο υπεύθυνος ιατρός που έχει αναλάβει τη θεραπεία του, κρίνει ότι στα πλαίσια της διάγνωσης θα πρέπει να πραγματοποιηθούν ακτινογραφικές εξετάσεις.

Μετά από μια πρώτη ανάλυση των ακτινογραφιών, ο ιατρός διακρίνει μια ύποπτη περιοχή . Στην προσπάθεια του να επιβεβαιώσει τα ευρήματά του, αποστέλλει τις πληροφορίες που αφορούν τον ασθενή οι οποίες συμπεριλαμβάνονται στον ηλεκτρονικό του φάκελο, σε έναν άλλο ιατρό σε μια χώρα εντός της Ευρωπαϊκής Ένωσης.

- *Ανάλυση παραδείγματος 1*

Σε αυτή την περίπτωση, παρατηρούμε μια κατάσταση στην οποία υπάρχει μεταφορά δεδομένων μεταξύ δύο επαγγελματιών υγείας που βρίσκονται σε διαφορετικές χώρες εντός της Ευρωπαϊκής Ένωσης.

Τα δεδομένα που αφορούν τον ασθενή Χ, έχουν συλλέγει με βάση αυτά που ορίζει η νομοθεσία καθώς ο ασθενής έχει συμφωνήσει για την πραγματοποίηση των ιατρικών εξετάσεων. Επιπλέον, μεταφορά των δεδομένων του ασθενή γίνεται εφικτή γιατί έχει δώσει τη συγκατάθεσή του. Ο νόμος συμφωνεί με τη μεταφορά των ευαίσθητων δεδομένων γιατί οι περιπτώσεις αυτές συμπεριλαμβάνονται στις εξαιρέσεις που προβλέπονται για τα ευαίσθητα δεδομένα.

Η επεξεργασία των ευαίσθητων δεδομένων επιτρέπεται σε αυτή τη περίπτωση να γίνει από τον ιατρό, για σκοπούς που αφορούν τη διάγνωση και τη προσπάθεια παροχής υπηρεσιών προς τον ασθενή. Ο ιατρός είναι νόμιμα εγγεγραμμένος και πρέπει να πραγματοποιεί την επεξεργασία των δεδομένων στα πλαίσια της μυστικότητας και της εμπιστευτικότητας. Η επεξεργασία, θα γίνει σύμφωνα με την τοπική νομοθεσία ή σύμφωνα με κανόνες που έχουν διατυπωθεί από κάποιο τοπικό οργανισμό.

Επιπρόσθετα, η οδηγία καλύπτει την ανταλλαγή των δεδομένων μεταξύ των δύο ιατρών, εφόσον τα δεδομένα τα οποία θα ανταλλαχθούν αφορούν διαγνωστικούς σκοπούς. Ο προσωπικός ιατρός του ασθενή, έχει τη νομική υποχρέωση να διασφαλίσει ότι ο παραλήπτης των δεδομένων και το ίδρυμα στο οποίο στεγάζεται, παρέχουν τις απαραίτητες εγγυήσεις ασφαλείας σε τεχνικό και οργανωτικό επίπεδο. Ο παραλήπτης με τη σειρά του θα πρέπει να επεξεργαστεί τα δεδομένα εκ μέρους του αποστολέα ιατρού και θα πρέπει να ακολουθεί τις οδηγίες που θα καθορίσει ο αποστολέας.

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία «προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες»): Η οδηγία 2002/58/ΕΚ αποτελεί μια οδηγία της Ευρωπαϊκής Ένωσης για την προστασία δεδομένων και της εμπιστευτικότητας στις ηλεκτρονικές επικοινωνίες. Συγκεκριμενοποιεί και συμπληρώνει την οδηγία 95/46/ΕΚ σε πολλά σημαντικά ζητήματα όπως είναι η μυστικότητα των πληροφοριών, η αποστολή ηλεκτρονικών μηνυμάτων, η αποστολή spam και η χρήση cookies.

Η οδηγία αυτή βρίσκει εφαρμογή στο χώρο του ηλεκτρονικού φακέλου ασθενή εφόσον οι ηλεκτρονικές επικοινωνίες θα αποτελέσουν την υποδομή του συστήματος. Μέσω των ηλεκτρονικών επικοινωνιών και συγκεκριμένα των δημοσίων δικτύων, θα ανταλλάζονται τα μηνύματα τα οποία περιέχουν πληροφορίες υγείας μεταξύ των διαφόρων συστημάτων υγείας, ώστε να επιτευχθεί ο σκοπός της διαλειτουργικότητας.

Το Διαδίκτυο έρχεται να ανατρέψει τις παραδοσιακές δομές των συστημάτων υγείας, παρέχοντας τη δυνατότητα μιας ενιαίας και παγκοσμίας υποδομής για την παροχή μιας πληθώρας υπηρεσιών υγείας με σκοπό την ποιοτικότερη και βελτιωμένη ιατρική περίθαλψη. Παρόλο που το Διαδίκτυο δημιουργεί καινούργιες δυνατότητες σε όλους τους φορείς της υγείας, η χρήση του εγκυμονεί κινδύνους για τα προσωπικά τους δεδομένα και την προστασία της ιδιωτικής τους ζωής.

Η οδηγία αυτή έχει δημιουργηθεί με σκοπό τη διευκόλυνση των ηλεκτρονικών υπηρεσιών και την εξέταση διάφορων ζητημάτων που έχουν σχέση με την ηλεκτρονική επικοινωνία καθώς και την προστασία της ιδιωτικής ζωής μέσω των ηλεκτρονικών υπηρεσιών. Κύριος σκοπός της είναι να

επιτραπεί η ελεύθερη κυκλοφορία των νόμιμα επεξεργασμένων προσωπικών δεδομένων μέσα στα κράτη της Ευρωπαϊκής Ένωσης. Θέτει επίσης τα θεμέλια της εμπιστευτικότητας ως θεμελιώδεις αρχές εφαρμόσιμες σε όλες τις μορφές ηλεκτρονικών επικοινωνιών.

Τα κράτη μέλη της Ευρωπαϊκής Ένωσης είναι υποχρεωμένα να προστατεύουν τα προσωπικά δεδομένα κάθε ατόμου και τις επικοινωνίες που γίνονται μέσω ενός δικτύου. Ειδικότερα, είναι υποχρεωμένα να μην επιτρέπουν σε κανένα την υποκλοπή και αποθήκευση προσωπικών δεδομένων κάποιου ατόμου εκτός βέβαια αν ο χρήστης στον οποίο ανήκουν τα δεδομένα έχει δώσει τη συγκατάθεσή του. Μαζί με τη γενική οδηγία προστασίας δεδομένων, η οδηγία για τη μυστικότητα και τις ηλεκτρονικές επικοινωνίες δημιουργούν ένα γενικό και ουδέτερο σύστημα τεχνολογίας της προστασίας δεδομένων σε όλα τα κράτη μέλη της Ε.Ε.

Η οδηγία 95/46/ΕΚ καλύπτει οποιαδήποτε μορφή επεξεργασίας των προσωπικών δεδομένων ανεξάρτητα από τη τεχνολογία η οποία χρησιμοποιείται. Τα προβλεπόμενα μέτρα για τις ηλεκτρονικές επικοινωνίες σε συνδυασμό με τους γενικούς κανόνες προστασίας των δεδομένων, δεν παρέχουν την κατάλληλη προστασία των δεδομένων ανεξάρτητα από την τεχνολογία που θα χρησιμοποιηθεί. Συνεπώς θα πρέπει να προβλεφθούν τα κατάλληλα μέτρα τα οποία θα αναγκάζουν τους κατασκευαστές του εξοπλισμού των ηλεκτρονικών επικοινωνιών να κατασκευάζουν προϊόντα τα οποία διασφαλίζουν την προστασία των προσωπικών δεδομένων των ατόμων, και συνεπώς θα διασφαλίζουν την προστασία των ιατρικών δεδομένων των ασθενών.

Σύμφωνα με την οδηγία 1999/5/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Μαρτίου 1999 σχετικά με το ραδιοεξοπλισμό και τον τηλεπικοινωνιακό τερματικό εξοπλισμό, θα εξασφαλίζει την εναρμόνιση της εισαγωγής τεχνικών χαρακτηριστικών εξοπλισμού ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένου του λογισμικού, για τους σκοπούς της προστασίας των δεδομένων.

Η οδηγία αυτή σε συνδυασμό με την γενική οδηγία της προστασίας των δεδομένων, θα διαδραματίσουν καθοριστικό ρόλο στην νομική επιτυχία του συστήματος ηλεκτρονικού φακέλου ασθενή. Εναρμόνιση του συστήματος με την οδηγία αυτή, θα του επιτρέψει να διαλειτουργήσει με συστήματα υγείας σε Ευρωπαϊκό επίπεδο. Ένα από τα βασικότερα οράματα της Ευρωπαϊκής Κοινότητας που αποδίδονται μέσα από την στρατηγική i2010, είναι η παροχή καλύτερων υπηρεσιών υγείας δια μέσου της χρήσης της τεχνολογίας και των ηλεκτρονικών επικοινωνιών.

Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα: Η οδηγία αυτή, έχει ως σκοπό να εναρμονίσει τις διατάξεις των κρατών μελών στην προσπάθεια διασφάλισης ενός επιπέδου προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών όσον αφορά την ιδιωτικότητα των δεδομένων στον τομέα της

επεξεργασίας και διακίνησης των δεδομένων στον τηλεπικοινωνιακό τομέα, συμπληρώνοντας την οδηγία 95/46/ΕΚ. Επιπλέον, παρέχεται προστασία των συμφερόντων των συνδρομητών σύμφωνα πάντα με τη νομοθεσία.

Μέσα από κάποιες εκτιμήσεις, τελικά παρουσιάστηκαν τα άρθρα αυτής της οδηγίας όπου δίνουν κάποιες κατευθυντήριες γραμμές σχετικά με τις υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής, την ασφάλεια και το απόρρητο των επικοινωνιών και γενικά την ασφάλεια της ιδιωτικότητας των ατόμων που χρησιμοποιούν τηλεπικοινωνίες.

Οι παροχείς τηλεπικοινωνιακών υπηρεσιών οφείλουν να λαμβάνουν τα κατάλληλα μέτρα, οργανωτικής και τεχνικής φύσης, προκειμένου να προστατεύουν την ασφάλεια των υπηρεσιών τους και την ασφάλεια του δικτύου τηλεπικοινωνιών. Θα πρέπει να χρησιμοποιούνται οι πιο πρόσφατες τεχνολογίες και δυνατότητες έτσι ώστε να εξασφαλίζεται το ικανοποιητικό επίπεδο ασφάλειας ως προς τους αντίστοιχους κινδύνους. Η χρήστες των τηλεπικοινωνιακών δικτύων, θα πρέπει να ενημερώνονται σε περιπτώσεις παραβίασης της ασφάλειας του δικτύου καθώς και για τρόπους αποφυγής τους.

Τα κράτη, μέσω εθνικών νομοθεσιών, κατοχυρώνουν το απόρρητο των επικοινωνιών που γίνονται μέσω δημόσιου τηλεπικοινωνιακού δικτύου και των τηλεπικοινωνιακών υπηρεσιών που είναι διαθέσιμες στο κοινό. Για παράδειγμα θα πρέπει να απαγορεύεται η υποκλοπή, ακρόαση, και η παρακολούθηση επικοινωνιών από μη εξουσιοδοτημένα πρόσωπα.

Η προηγούμενη οδηγία 2002/58/ΕΚ αποτελεί ένα υπερσύνολο της οδηγίας αυτής και μαζί θωρακίζουν την ασφάλεια των δικτύων εφόσον εφαρμόζονται οι αρχές που καθορίζονται.

Σύσταση Αρ.R (81) 1 της επιτροπής των υπουργών προς τα κράτη μέλη για κανονισμούς για αυτοματοποιημένες τράπεζες ιατρικών δεδομένων: Η σύσταση αυτή, περιλαμβάνει κάποιες αρχές σχετικά με την αυτοματοποιημένη οργάνωση ιατρικών δεδομένων σε βάσεις πληροφοριών. Κάθε αυτοματοποιημένη ιατρική τράπεζα , πρέπει να υπόκειται σε συγκεκριμένους κανονισμούς, σύμφωνα πάντα με τους νόμους του συγκεκριμένου κράτους όπου διατηρείται.

Οι τράπεζες αυτές θα πρέπει να διαφυλάσσουν τα ατομικά δικαιώματα και ελευθερίες των ασθενών. Μια ιατρική τράπεζα μπορεί να συνδυάζει διάφορα σύνολα ιατρικών αναφορών ή διάφορα είδη ιατρικών δεδομένων, με αποτέλεσμα κάθε ένα από αυτά τα δεδομένα να μπορεί να απαιτήσει ξεχωριστούς κανονισμούς σχετικά με τα επιπρόσθετα χαρακτηριστικά γνωρίσματά του. Ήταν η πρώτη οδηγία η οποία παρουσίασε διεθνές ενδιαφέρον για το θέμα αυτό θέτοντας παράλληλα τα απαραίτητα μέτρα μέσω των οποίων θα ήταν δυνατή η πρόσβαση του ατόμου στα δεδομένα του μέσω του ιατρού.

Σύσταση Αρ. R(83) 10 για την προστασία των προσωπικών δεδομένων τα οποία χρησιμοποιούνται για επιστημονική έρευνα και στατιστικές: Αυτή η σύσταση παρέχει αρχές και

οδηγίες οι οποίες πρέπει να ισχύουν σχετικά με τη χρήση των προσωπικών δεδομένων για την επιστημονική έρευνα και στατιστικές τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Ανεξάρτητα από το αν η επεξεργασία των προσωπικών στοιχείων είναι αυτοματοποιημένη ή μη.

Η σύσταση, σέβεται τους κανόνες της εμπιστευτικότητας του κάθε ατόμου του οποίου τα δεδομένα απαιτούνται να αποτελέσουν αντικείμενο έρευνας. Πολύ σημαντικό στην οδηγία αυτή είναι το γεγονός ότι, τονίζεται πως η έρευνα θα πρέπει να γίνεται εάν αυτό καθίσταται εφικτό, με ανώνυμα δεδομένα. Έχοντας αυτή την αρχή υπόψη, η οδηγία αυτή καλεί επιστημονικούς και επαγγελματικούς οργανισμούς, καθώς και αρχές σχετικά με το δημόσιο τομέα, να προωθούν την ανάπτυξη ασφαλών τεχνικών και διαδικασιών που θα σέβονται την ανωνυμία.

Οποιοσδήποτε παρέχει δεδομένα τα οποία θα λάβουν μέρος σε διαδικασίες έρευνας, πρέπει να ενημερώνεται πλήρως για το σκοπό και τους στόχους της έρευνας καθώς και για τα στοιχεία του οργανισμού ο οποίος είναι υπεύθυνος για τη διεξαγωγή της έρευνας. Πρέπει να διατηρείται το δικαίωμα του ατόμου που έδωσε τα στοιχεία, να αποσύρει τα δεδομένα του σε οποιαδήποτε στιγμή χωρίς να δώσει οποιοδήποτε λόγο.

Προβλέπονται επιπρόσθετα μέτρα προστασίας σχετικά με τα πρόσωπα από τα οποία συλλέγονται στοιχεία και τα οποία δεν είναι σε θέση να δώσουν τη συγκατάθεσή τους ελεύθερα όπως για παράδειγμα ασθενείς οι οποίοι βρίσκονται σε κωματώδη κατάσταση.

Σχετικά με τη χρήση των δεδομένων, προβλέπεται ότι τα δεδομένα τα οποία χρησιμοποιούνται για μια συγκεκριμένη έρευνα, δεν μπορούν να χρησιμοποιηθούν για οποιοδήποτε άλλο σκοπό εκτός από τον συγκεκριμένο. Στην περίπτωση όπου δεν υπάρχει χρόνος για την συλλογή δεδομένων για έναν ερευνητικό σκοπό και δεδομένου ότι η ο ερευνητής καλύπτεται από την τοπική νομοθεσία, μπορεί να χρησιμοποιήσει δεδομένα τα οποία έχει στην κατοχή του από προηγούμενες διεξαγωγές ερευνών.

Το δημόσιο ή ιδιωτικοί οργανισμοί, μπορούν να γνωστοποιήσουν στοιχεία τα οποία αποτελούν προσωπικά δεδομένα, μόνο με τη συγκατάθεση του ατόμου που αφορούν τα συγκεκριμένα δεδομένα για έρευνα. Το δικαίωμα του ατόμου που έδωσε τα στοιχεία για να διορθώσει και να έχει πρόσβαση στα δεδομένα του, μπορεί να μην ισχύει σε περιπτώσεις που η επεξεργασία γίνεται χωρίς την πιθανότητα αναγνώρισης του συγκεκριμένου ατόμου. Επιπλέον, μπορεί να μην ισχύει σε περιπτώσεις όπου υπάρχουν οι απαραίτητες εγγυήσεις ως προς την ασφάλεια σε κάθε στάδιο της έρευνας.

Όσον αφορά την ασφάλεια των δεδομένων, οι οργανισμοί πρέπει να διασφαλίζουν ότι οι λαμβάνονται τα κατάλληλα μέτρα ασφαλείας, τόσο σε διοικητικό επίπεδο όσο και σε τεχνικό επίπεδο. Η δημοσίευση πληροφοριών που αφορούν την έρευνα, πρέπει να γίνεται με τρόπο με τον οποίο να αποτρέπεται η αναγνώριση ενός προσώπου που έλαβε μέρος στην έρευνα, εκτός και αν έχει δοθεί η συγκατάθεσή του.

Η σύσταση, καθορίζει ότι με την ολοκλήρωση του έργου, τα δεδομένα πρέπει να καταστρέφονται ή σε περιπτώσεις που έγινε ανώνυμη έρευνα να μπορούν να διατηρούνται κάτω από συγκεκριμένους κανόνες που θα οριστούν.

Η οδηγία αυτή, δίνει σαφείς οδηγίες για το πώς θα χρησιμοποιούνται τα δεδομένα του ηλεκτρονικού φακέλου ασθενή για έρευνα στα πλαίσια των δευτεροβάθμιων χρήσεων των ηλεκτρονικών φακέλων ασθενών έτσι ώστε να διασφαλίζεται η προστασία της ιδιωτικότητας και της εμπιστευτικότητας.

Σύσταση Αρ.R (99) 5 της επιτροπής των υπουργών προς τα κράτη μέλη για την προστασία της ιδιωτικότητας στο Internet: Το διαδίκτυο παρέχει πολλά πλεονεκτήματα όταν χρησιμοποιείται για την ανταλλαγή των δεδομένων και την αλληλεπίδραση μεταξύ των παρόχων υπηρεσιών υγείας, των ασθενών, και των ερευνητών όπως γίνεται στον ηλεκτρονικό φάκελο ασθενή. Εντούτοις, τα πλεονεκτήματα που παρέχονται από το Διαδίκτυο συνεπάγονται αυξημένους κινδύνους όσον αφορά την εμπιστευτικότητα, την ακεραιότητα, και τη διαθεσιμότητα των πληροφοριών. Είναι ουσιαστικό τα ιδρύματα υγειονομικής περίθαλψης που επεξεργάζονται και που ανταλλάσσουν τα ιατρικά δεδομένα να χρησιμοποιούν μια κατάλληλη πολιτική ασφαλείας.

Η σύσταση αυτή, έρχεται να δώσει τις κατευθυντήριες αρχές που αφορούν τη συλλογή και την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο Διαδίκτυο. Αναγνωρίζεται η ανάγκη για διασφάλιση της ανωνυμίας και της εμπιστευτικότητας καθώς ανταλλάζονται πληροφορίες, έτσι ώστε να διασφαλίζονται τα θεμελιώδη δικαιώματα και ελευθερίες του ατόμου όπως αυτές ορίζονται από το άρθρο 8 της ευρωπαϊκής σύμβασης για τα ανθρώπινα δικαιώματα.

Συμβούλιο της Ευρώπης, Επιτροπή των Υπουργών, Σύσταση Αρ. R (97) 5 για την προστασία των ιατρικών δεδομένων: Αυτή η σύσταση, μπορεί να λειτουργήσει σε περίπτωση που δεν υπάρχει κρατική ρύθμιση που να αφορά τη διαφύλαξη των προσωπικών δεδομένων. Μέσω αυτής της σύστασης λαμβάνονται υπόψη οι θεμελιώδεις αρχές διαφύλαξης των ιατρικών δεδομένων. Σε γενικές γραμμές, τα ιατρικά δεδομένα πρέπει να συλλέγονται και να διατηρούνται από ειδικούς παροχείς ιατρικής περίθαλψης ή οργανισμούς που δουλεύουν εκ μέρους ειδικών σε θέματα υγείας. Η συλλογή και επεξεργασία των δεδομένων, μπορεί να γίνει εφόσον ο νόμος το επιτρέπει για λόγους δημοσίας υγείας ή άλλους σημαντικούς λόγους που αφορούν το δημόσιο συμφέρον. Επίσης, τα δεδομένα υγείας μπορούν να χρησιμοποιηθούν για διαγνωστικούς σκοπούς ή για διατήρηση αρχείου του ιατρού.

Σύμφωνα με τη σύσταση, ο ασθενής διατηρεί το δικαίωμα ενημέρωσης σχετικά με την ύπαρξη ενός φακέλου που περιέχει το ιατρικό του ιστορικό και τον τύπο των πληροφοριών που διατηρούνται σε αυτόν.

Κάθε άτομο έχει το δικαίωμα να έχει πρόσβαση στα προσωπικά του δεδομένα, είτε άμεσα είτε μέσω ενός παρόχου υγείας. Η πληροφορίες πρέπει να βρίσκονται σε κατανοητή μορφή έτσι

ώστε να μπορεί κάποιος να τις αντιληφθεί. Τα δεδομένα που βρίσκονται στο αρχείο του ασθενή μπορούν να χρησιμοποιηθούν για στατιστικούς σκοπούς ή σκοπούς έρευνας δεδομένου ότι δεν υπάρχει καμία ένδειξη ότι θα πραγματοποιηθεί παραβίαση της ασφάλειας των δεδομένων.

Επιπρόσθετα, καθορίζει ότι πρέπει να λαμβάνονται τα κατάλληλα μέτρα έτσι ώστε να διασφαλίζεται η μη απώλεια δεδομένων και ότι κανένα μη εξουσιοδοτημένο πρόσωπο δεν θα έχει πρόσβαση σε αυτά για να πραγματοποιήσει οποιαδήποτε επεξεργασία. Επιπλέον, ορίζει ότι πρέπει να διασφαλίζονται οι χώροι αποθήκευσης των δεδομένων και να μην επιτρέπεται η μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα των νοσοκομείων.

Σημαντικό στοιχείο αναφοράς είναι ότι μέσα από αυτή τη σύσταση, δηλώνεται ότι πρέπει να γίνεται διαχωρισμός ανάμεσα στα δεδομένα τα οποία βρίσκονται στο φάκελο του ασθενή. Δηλαδή, να υπάρχει διαχωρισμός ανάμεσα στα αναγνωριστικά δεδομένα της ταυτότητας ενός προσώπου, στα διοικητικά δεδομένα, στα δεδομένα υγείας, στα κοινωνικά, δημογραφικά δεδομένα και στα γενετικά δεδομένα, κάτι το οποίο θα πρέπει να ισχύει και στην περίπτωση του ηλεκτρονικού φακέλου ασθενή.

Ξεκίνησε από την περιοχή της γενετικής και αποτελούσε μια προσπάθεια να τεθούν τα πρότυπα για τη διαχείριση των ιατρικών δεδομένων έτσι ώστε οι ασθενείς να μπορούν να νιώθουν σίγουροι ότι τα δεδομένα που τους αφορούν δεν θα είναι εκτεθειμένα στον κίνδυνο αλλά θα προστατεύονται.

Κανονισμός Αρ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου 2000 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών: Σκοπός αυτού του κανονισμού είναι η διασφάλιση τόσο της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των ατόμων, όσο και της ελευθερίας των προσωπικών δεδομένων μεταξύ των μελών και των οργάνων της Ευρωπαϊκή Ένωσης όπου εφαρμόζουν την οδηγία 95/46/ΕΚ. Η επεξεργασία των προσωπικών δεδομένων γίνεται με σκοπό την εφαρμογή του κοινοτικού δικαίου.

Ο κανονισμός αυτός έχει εφαρμογή για την επεξεργασία προσωπικών δεδομένων από όλα τα όργανα της Ευρωπαϊκής Ένωσης. Εφαρμόζεται επίσης τόσο για την αυτοματοποιημένη, όσο και για τη μη αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων τα οποία δεδομένα θα πρέπει να περιληφθούν σε κάποιο αρχείο.

Τα δεδομένα θα πρέπει να συλλέγονται ,να επεξεργάζονται και να διατηρούνται κάτω από τους κανόνες που ορίζει νομοθεσία για τους συγκεκριμένους σκοπούς. Θα πρέπει να χαρακτηρίζονται από ακρίβεια, πληρότητα και συνάφεια και να ενημερώνονται όποτε αυτό καθίσταται αναγκαίο. Επίσης, τα δεδομένα θα πρέπει να διατηρούνται με τέτοια μορφή, έτσι ώστε να είναι δυνατή η ταυτοποίηση του συγκεκριμένου ατόμου μόνο για το αναγκαίο χρονικό διάστημα που τίθεται. Τα

διάφορα όργανα όμως θα πρέπει να προνοήσουν για προσωπικά δεδομένα τα οποία θα πρέπει να αποθηκευτούν για μεγαλύτερο χρονικό διάστημα από το αναγκαίο, για στατιστικούς, ιστορικούς και ερευνητικούς σκοπούς μόνο. Τα δεδομένα αυτά πρέπει να διατηρούνται με τέτοια μορφή έτσι ώστε να αποκρύπτεται η ταυτότητα του ατόμου, και αν αυτό δεν καθίσταται δυνατόν, θα πρέπει η ταυτότητα του ατόμου να έχει κρυπτογραφική μορφή.

Η διαβίβαση των προσωπικών δεδομένων ενός ατόμου στο εσωτερικό ή μεταξύ οργάνων της Κοινότητας, επιτρέπεται μόνον εφόσον τα δεδομένα είναι απαραίτητα για την εκτέλεση νόμιμων καθηκόντων που εμπίπτουν στην αρμοδιότητα του αποδέκτη. Το άτομο ή οργανισμός όπου θα επεξεργαστεί τα δεδομένα, θα πρέπει να τα επεξεργαστεί , μόνο για τους σκοπούς για τους οποίους τα έχει εξασφαλίσει . Η διαβίβαση τους όμως σε χώρες εκτός της Κοινότητας, οι οποίες δεν εφαρμόζουν την οδηγία 95/46/EC, είναι επιτρεπτή μόνο εάν μπορεί να εξασφαλιστεί το επαρκές επίπεδο προστασίας.

Η επεξεργασία ευαίσθητων προσωπικών δεδομένων απαγορεύεται εκτός και αν ισχύουν κάποιοι κανονισμοί. Η επεξεργασία σε μια τέτοια περίπτωση είναι δυνατή, εφόσον το άτομο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεσή του, ή όταν η επεξεργασία κρίνεται απαραίτητη για τη διατήρηση ζωτικών συμφερόντων του συγκεκριμένου ατόμου ή κάποιου άλλου ατόμου όταν το άτομο στο οποίο αναφέρονται τα δεδομένα, δεν μπορεί να δώσει τη συγκατάθεσή του. Ακόμη, η επεξεργασία είναι δυνατή εάν για παράδειγμα τα δεδομένα είναι απαραίτητα για υπεράσπιση του στο δικαστήριο. Η επεξεργασία μπορεί να πραγματοποιηθεί όταν υπάρχει ανάγκη για ιατρική διάγνωση για τον ασθενή και γενικά για την παροχή υπηρεσιών υγείας από άτομα τα οποία είναι υποχρεωμένα να διατηρήσουν το επαγγελματικό απόρρητο, όπως για παράδειγμα οι ιατροί οι οποίοι είναι υποχρεωμένοι να διασφαλίσουν το ιατρικό απόρρητο.

Για την επεξεργασία των προσωπικών δεδομένων, θα πρέπει να λαμβάνονται και τα κατάλληλα μέτρα για τη διατήρηση της ασφάλειας και της προστασίας τους. Όταν τα δεδομένα υπόκεινται σε αυτοματοποιημένη επεξεργασία, θα πρέπει να λαμβάνονται μέτρα έτσι ώστε να αποτρέπουν ένα άτομο το οποίο δεν έχει την ανάλογη εξουσιοδότηση, να έχει πρόσβαση στα διάφορα πληροφοριακά συστήματα τα οποία χρησιμοποιούνται για την επεξεργασία. Να καθίσταται μη επιτρεπτή η εισαγωγή, ανάγνωση, διαγραφή ακόμη και η διαβίβαση των προσωπικών δεδομένων. Οι εξουσιοδοτημένοι δε χρήστες, δεν πρέπει να διαθέτουν πρόσβαση σε άλλα δεδομένα προσωπικού χαρακτήρα εκτός από εκείνα που καλύπτονται από το δικαίωμα πρόσβασης που τους παρέχεται. Θα πρέπει να καταγράφονται τα ίχνη των προσωπικών δεδομένων τα οποία έχουν ανακοινωθεί, η χρονική στιγμή της ανακοίνωσης και ο αποδέκτης τους.

Στην περίπτωση όπου η επεξεργασία των προσωπικών δεδομένων γίνεται με τη χρήση τηλεπικοινωνιακών δικτύων ή ηλεκτρονικών υπολογιστών, θα πρέπει επίσης να διασφαλίζεται η εμπιστευτικότητα και η ασφάλεια των δεδομένων. Όταν για παράδειγμα η ασφάλεια του δικτύου τίθεται σε κίνδυνο, οι χρήστες του θα πρέπει να ενημερώνονται κατάλληλα και να δίνονται κάποιοι εναλλακτικοί τρόποι επικοινωνίας, καθώς και μέτρα για να αποφευχθεί ο κίνδυνος.

3.4.2 Ευρωπαϊκός Χάρτης για τα δικαιώματα των ασθενών

Με τη δημιουργία αυτού του Χάρτη σε συνδυασμό με τον Χάρτη των Θεμελιωδών Δικαιωμάτων, η Ευρωπαϊκή Ένωση θέλει να τονίσει ότι όλοι οι πολίτες της έχουν ίσα δικαιώματα στην ιατρική περίθαλψη και δεν μπορούν να αμφισβητηθούν, ειδικά για οικονομικούς λόγους. Αυτός ο οικονομικός παράγοντας δεν μπορεί να νομιμοποιήσει ή να αρνηθεί τα δικαιώματα που έχουν όλα τα άτομα να τύχουν ιατρικής περίθαλψης.

Επίσης γνωρίζοντας ότι πολλά από τα δικαιώματα των ασθενών καταπατούνται, μέσα στα οποία συγκαταλέγονται η πρόσβαση στα ιατρικά τους δεδομένα, η ιατρική τους πληροφόρηση, η εμπιστευτικότητα και η μυστικότητα, ο Χάρτης αυτός αποσκοπεί στο να αποτελέσει τη βάση για την εξάλειψη αυτής της καταπάτησης. Αξίζει να σημειωθεί το γεγονός ότι τα δικαιώματα αυτά ισχύουν ακόμη και όταν ένα κράτος δεν έχει υλοποιημένο κάποιο σχετικό νόμο.

Ο ευρωπαϊκός αυτός Χάρτης θα έχει ισχύ σε όλα τα κράτη μέλη ανεξάρτητα από τη διαφορετικότητα που ίσως να διαθέτουν τα διάφορα συστήματα υγείας μεταξύ τους. Ανεξάρτητα ακόμη και του τι βρίσκεται υλοποιημένο σε κάθε χώρα σχετικά με το ευρύτερο θέμα της υγείας του ασθενή όπως για παράδειγμα αν έχουν υλοποιήσει ή όχι κάποιους συγκεκριμένους νόμους για τους ασθενείς, κάποιες υπηρεσίες κτλ. Έτσι, γνωρίζοντας ότι επιτρέπεται η ελεύθερη διακίνηση των δεδομένων στις χώρες τις ΕΕ, το επίπεδο προστασίας και ασφάλειας των ασθενών θα αυξηθεί.

Η υλοποίηση του Χάρτη αρχικά θα γίνει στα κράτη τα οποία έχουν υλοποιημένα τα δικαιώματα των ασθενών σε ένα εθνικό επίπεδο με τη δέσμευση πάντα της κυβέρνησης, των παροχών ιατρικής περίθαλψης και της νομοθεσίας. Όταν γίνει η εφαρμογή του Χάρτη, θα πρέπει όλα τα κράτη μέλη να τροποποιήσουν το νομοθετικό τους πλαίσιο έτσι ώστε να προσαρμοστεί με το Χάρτη χωρίς όμως να μην λαμβάνεται υπόψη η εθνική νομοθεσία όταν αυτή προσφέρει μεγαλύτερο επίπεδο ασφάλειας.

Μέσα από αυτόν τον Χάρτη καθορίζονται δεκατέσσερα θεμελιώδη δικαιώματα για τους ασθενείς με σκοπό πάντα την προστασία και την ασφάλεια της υγείας των πολιτών, και είναι τα ακόλουθα:

- Δικαίωμα στην πληροφόρηση
- Δικαίωμα στην πρόσβαση
- Δικαίωμα στην ελεύθερη επιλογή

- Δικαίωμα στην ιδιωτική ζωή και στην εμπιστευτικότητα
- Δικαίωμα στην ασφάλεια
- Δικαίωμα στην πρόληψη
- Δικαίωμα στην συγκατάθεση
- Δικαίωμα στο χρόνο των ασθενών
- Δικαίωμα στην τήρηση των ποιοτικών προτύπων
- Δικαίωμα στην καινοτομία
- Δικαίωμα της αποφυγής του περιττού πόνου και βασάνου
- Δικαίωμα στην εξατομικευμένη επεξεργασία
- Δικαίωμα του ατόμου να παραπονεθεί
- Δικαίωμα της αποζημίωσης.

➢ *Δικαίωμα στην πρόσβαση*

Κάθε άτομο έχει το δικαίωμα να εξυπηρετηθεί από οποιαδήποτε υπηρεσία υγείας, με ίση εξυπηρέτηση από την κάθε μία, με βάση τις ανάγκες του. Ακόμη και αν αυτό το άτομο δεν μπορεί να πληρώσει τα έξοδα που του επιβάλλονται, μπορεί να εξυπηρετηθεί δωρεάν. Επίσης κάθε άτομο το οποίο βρίσκεται σε μια χώρα, χωρίς απαραίτητα να διαμένει εκεί, έχει το δικαίωμα στην επείγουσα ιατρική περίθαλψη. Ακόμη κάποιο άτομο το οποίο υποφέρει από κάποια σπάνια ασθένεια έχει το δικαίωμα ίσης περίθαλψης με κάποιο που υποφέρει από μια συνήθης ασθένεια.

➢ *Δικαίωμα πληροφόρησης*

Κάθε άτομο έχει το δικαίωμα πρόσβασης στον ιατρικό του φάκελο και τις ιατρικές του αναφορές, να πάρει κάποιο αντίτυπό του και να το διορθώσει εάν κρίνει ότι κάποια πληροφορία η οποία διατηρείται είναι λανθασμένη. Επίσης κάθε άτομο έχει το δικαίωμα πρόσβασης στην πληροφορία για ερευνητικούς σκοπούς ή για ιατροφαρμακευτική περίθαλψη εφόσον πρώτα επιβεβαιωθεί η ακρίβεια και η διαφάνεια.

➢ *Δικαίωμα ιδιωτικής ζωής και εμπιστευτικότητας*

Κάθε άτομο έχει δικαίωμα της εμπιστευτικότητας της πληροφορίας σχετικά με οποιοδήποτε θέμα σχετίζεται με την υγεία του. Από τις πληροφορίες σχετικά με μια ασθένεια μέχρι μια θεραπεία. Οι πληροφορίες αυτές είναι άκρως εμπιστευτικές και προστατευμένες.

Υπάρχουν αρκετά διεθνή έγγραφα από τον οργανισμό WHO και το Ευρωπαϊκό Συμβούλιο, ανάμεσα στα οποία συγκαταλέγονται και η Διακήρυξη όσον αφορά την προώθηση των δικαιωμάτων των ασθενών στην Ευρώπη, στο Άμστερνταμ το 1994.

3.5 Νομοθετικό Πλαίσιο για Ηνωμένες Πολιτείες της Αμερικής – HIPAA

Ο νόμος Health Insurance Portability and Accountability Act(HIPAA) θεσπίστηκε από το Αμερικανικό Κογκρέσο το 1996. Σκοπός της θέσπισής του ήταν ο περιορισμός της δυνατότητας άρνησης των εργοδοτών για προσφορά ασφαλιστικής κάλυψης σε εργαζομένους με προηγούμενα προβλήματα υγείας. Αποτέλεσμα αυτού του νόμου είναι η διασφάλιση της ιδιωτικότητας του ασθενή. Μια αρχή της HIPAA είναι η προστασία του πολίτη δίνοντας του δικαίωμα να λάβει τον προσωπικό ηλεκτρονικό του φάκελο, να ζητήσει τροποποιήσεις στον φάκελο του και να ενημερωθεί σε ποια άτομα γνωστοποιήθηκαν προσωπικές πληροφορίες που εμπεριέχονταν στον φάκελο του.

Τα πρότυπα ασφάλειας της HIPAA ισχύουν για τις προστατευμένες ιατρικές πληροφορίες που είτε αποθηκεύονται είτε μεταφέρονται ηλεκτρονικά. Προστατευμένες (Protected Health Information) είναι αυτές οι πληροφορίες που οδηγούν στην αναγνώριση της ταυτότητας του ασθενούς δηλαδή τα ευαίσθητα προσωπικά δεδομένα.

Στην Αμερική το 2003 θεσμοθετήθηκε η νομική υποχρέωση της προάσπισης της ιδιωτικότητας και της εμπιστευτικότητας των δεδομένων του ασθενή υπό την αιγίδα του HIPAA. Οι κανονισμοί HIPAA θέτουν τις αρχές και τις διαδικασίες για την εξασφάλιση ότι η αποκάλυψη προσωπικών δεδομένων θα μειωθεί στο ελάχιστο δυνατό.

- *Κανόνας Transaction and Code Set*

Με τον όρο συναλλαγές ορίζονται ανταλλαγές ηλεκτρονικής μορφής που περιλαμβάνουν τη μεταφορά των πληροφοριών υγειονομικής περίθαλψης μεταξύ δύο οντοτήτων για συγκεκριμένους σκοπούς, όπως για παράδειγμα ένας παροχέας υπηρεσιών υγείας που υποβάλλει τις ιατρικές του αξιώσεις (claim) σε ένα σχέδιο υγείας για πληρωμή. Η HIPAA ονομάζει ορισμένους τύπους οργανώσεων ως καλυμμένες οντότητες, όπως είναι τα σχέδια υγείας και ορισμένοι παροχείς υπηρεσιών υγείας.

Η HIPAA υιοθέτησε επίσης ορισμένες τυποποιημένες συναλλαγές που αφορούν τον τρόπο ηλεκτρονικής ανταλλαγής δεδομένων, και συγκεκριμένα τη διαβίβαση δεδομένων υγειονομικής περίθαλψης μέσω του πρωτοκόλλου EDI (Electronic Data Interchange).

Τέτοιες συναλλαγές είναι: αιτήσεις για πληρωμές, συμβουλές πληρωμής, παραπομπές και εγκρίσεις, πληρωμές ασφαλίστρων. Εάν μια καλυμμένη οντότητα εκτελεί μια από τις επιτρεπτές συναλλαγές, πρέπει να συμμορφώνεται με τα πρότυπα που έχουν υιοθετηθεί και καθιερωθεί από το HIPAA. Αυτό σημαίνει ότι πρέπει να ακολουθεί τις απαιτήσεις περιεχομένου και σχήματος που διευκρινίζονται στα πρότυπα HIPAA.

Η HIPAA καθορίζει την μορφή των μηνυμάτων και δεδομένων που ανταλλάζονται μεταξύ των καλυμμένων οντοτήτων. Απαιτεί ότι κάθε καλυμμένη οντότητα χρησιμοποιεί συγκεκριμένες

κωδικοποιήσεις για τον προσδιορισμό των διαγνώσεων και των συγκεκριμένων κλινικών διαδικασιών που βρίσκονται για παράδειγμα στις αιτήσεις πληρωμής που απευθύνονται στις ασφαλιστικές εταιρείες. Παραδείγματα επιτρεπτών προτύπων που ορίζονται για διαγνώσεις και διαδικασίες είναι:

- Τα HCPCS (βοηθητικές υπηρεσίες/διαδικασίες),
- cpt-4 (διαδικασίες παθολόγων),
- CDT (οδοντική ορολογία),
- icd-9 (διαγνώσεις και διαδικασίες νοσοκομείου),
- icd-10 (εισαγωγή από την 1η Οκτωβρίου 2013) και
- NDC (εθνικοί κώδικες φαρμάκων)

Επιπλέον το HIPAA έχει υιοθετήσει πρότυπα για μοναδικά προσδιοριστικά για τους εργοδότες αλλά και τους παροχείς.

- *Security Rule*

Ο Security Rule, ασχολείται με τις ηλεκτρονικά προστατευμένες (EPHI) πληροφορίες υγείας. Δίνει κατευθυντήριες γραμμές που ασχολούνται με την ασφάλεια σε επίπεδο διοικητικό, φυσικό και τεχνικό.

Διοικητικό επίπεδο: Οι καλυμμένες οντότητες πρέπει να υιοθετήσουν ένα γραπτό σύνολο διαδικασιών μυστικότητας και να υποδείξουν έναν ανώτερο υπάλληλο που θα είναι ο αρμόδιος για την ανάπτυξη και εφαρμογή όλων των απαραίτητων πολιτικών και διαδικασιών. Οι πολιτικές και οι διαδικασίες πρέπει να αναφέρονται στις κατάλληλες αλλαγές που πρέπει να γίνουν ώστε οι οργανισμοί να διατηρούν τα κατάλληλα επίπεδα ασφαλείας.

Οι διαδικασίες πρέπει να προσδιορίσουν τους υπαλλήλους ή τις κατηγορίες υπαλλήλων που θα έχουν πρόσβαση στις ηλεκτρονικές προστατευμένες πληροφορίες υγείας (EPHI). Η πρόσβαση θα πρέπει να περιοριστεί μόνο σε εκείνους τους υπαλλήλους που χρειάζονται τις πληροφορίες για να διεκπεραιώσουν τη λειτουργία εργασίας τους.

Οι διαδικασίες πρέπει να εξετάσουν την έγκριση, την καθιέρωση, την τροποποίηση, και τη διακοπή πρόσβασης. Για να γίνει η ανταλλαγή δεδομένων από ένα πάροχο σε άλλο θα πρέπει να εξασφαλίζεται ότι οι παροχείς συμμορφώνονται με τις απαιτήσεις του HIPAA.

Πρέπει να λαμβάνονται τα κατάλληλα μέτρα ώστε να αποτρέπεται η απώλεια δεδομένων σε έκτακτες ανάγκες. Οι οργανισμοί οφείλουν να διατηρούν εφεδρική αποθήκευση των δεδομένων (backup) και σε περιπτώσεις που έλαβε χώρα μια καταστροφή να ακολουθούν συγκεκριμένες διαδικασίες για ανάκαμψη δεδομένων (data recovery).

Οι εσωτερικοί έλεγχοι (audit trail) διακατέχουν βασικό ρόλο στη HIPAA και είναι ένα μέτρο που αποτρέπει πιθανές παραβιάσεις. Έτσι, πρέπει να ακολουθούνται πολιτικές οι οποίες θα

εκτελούνται σε καθορισμένα χρονικά διαστήματα ή σε ένα απαραίτητο χρονικό διάστημα για αποκάλυψη τυχόν προβλημάτων ασφαλείας.

Φυσικό επίπεδο: Στο φυσικό επίπεδο ελέγχεται η φυσική πρόσβαση για την προστασία της πρόσβασης στα προστατευμένα δεδομένα. Πρέπει να υπάρχουν έλεγχοι για την εισαγωγή και την αφαίρεση του υλικού και του λογισμικού από το δίκτυο.

Η πρόσβαση στον εξοπλισμό που περιέχει τις πληροφορίες υγείας (π.χ. servers) πρέπει να ελεγχθεί προσεκτικά και να επιτηρηθεί. Η πρόσβαση στο υλικό και το λογισμικό πρέπει να περιοριστεί στα κατάλληλα εξουσιοδοτημένα άτομα. Επιπλέον, απαιτούνται πολιτικές για την κατάλληλη χρήση τερματικών σταθμών.

Τεχνικό επίπεδο: Στο τεχνικό επίπεδο, δίνονται κατευθυντήριες γραμμές για τον έλεγχο της πρόσβασης στα ηλεκτρονικά συστήματα, και αρχές για την προστασία των επικοινωνιών μέσω των οποίων διαβιβάζονται οι ηλεκτρονικές πληροφορίες δια μέσου δικτύων.

Τα πληροφοριακά συστήματα πρέπει να προστατευθούν από εισβολές. Όταν οι πληροφορίες διακινούνται δια μέσου δικτύου, θα πρέπει να ακολουθείται κάποια μορφή κρυπτογράφησης. Κάθε καλυμμένη οντότητα είναι αρμόδια για να εξασφαλίσει ότι τα δεδομένα που βρίσκονται αποθηκευμένα στα συστήματά του ηλεκτρονικού φακέλου ασθενή, δεν έχουν αλλάξει ή έχουν διαγραφεί με μη εξουσιοδοτημένο τρόπο.

Σύμφωνα με τη HIPAA, μπορούν να χρησιμοποιηθούν τεχνικές όπως είναι το checksum, double-Keying, επικύρωση μηνυμάτων, και ψηφιακές υπογραφές οι οποίες θα εξασφαλίσουν την ακεραιότητα των δεδομένων. Επιπρόσθετα, πρέπει να χρησιμοποιούνται τεχνικές επικύρωσης για την πιστοποίηση της ταυτότητα των συμμετεχόντων σε μια συναλλαγή. Παραδείγματα τέτοιων τεχνικών είναι: συστήματα κωδικού πρόσβασης, double or triple handshaking και token systems.

Ταυτόχρονα, ορίζει ότι θα πρέπει να πραγματοποιείται risk-analysis για την ανάλυση των πιθανών κινδύνων και πως αυτοί θα αντιμετωπίζονται. Με το risk-analysis, διασφαλίζεται ότι διατηρούνται οι απαιτήσεις ασφαλείας που ορίζονται από τη HIPAA στο κατώτατο επίπεδο.

- *Ερευνητικοί σκοποί*

Σύμφωνα με τις νομοθετικές ρυθμίσεις της HIPAA, οι ιατρικές πληροφορίες δεν πρέπει να αποκαλύπτονται χωρίς την συγκατάθεση του ασθενή, εκτός εάν απαιτείται η αποκάλυψη τους κάτω από ειδικές συνθήκες, όπως για ερευνητικούς σκοπούς. Η συναίνεση που απαιτείται για την αποκάλυψη των προσωπικών πληροφοριών του ασθενή εξαρτώνται από την αιτία της αποκάλυψής τους. Έτσι για την αποκάλυψη πληροφοριών, οι οποίες είναι απαραίτητες για τον καθορισμό της θεραπείας, της χρέωσης και της κάλυψης των υπηρεσιών για την παροχή φροντίδας του ατόμου, απαιτείται μια απλή, γενική συναίνεση από τον ίδιο τον ασθενή.

Σύμφωνα με τη HIPAA και τον κανονισμό Unique Identifiers Rule, καθορίζεται πως στις ηλεκτρονικές συναλλαγές θα πρέπει να χρησιμοποιείται μόνο το National Provider Identifier, για τον προσδιορισμό των συμβαλλόμενων μερών αντικαθιστώντας τα μέχρι τώρα αναγνωριστικά. Το National Provider Identifier, είναι ένα αλφανουμερικό αναγνωριστικό μήκους 10 ψηφίων με το τελευταίο ψηφίο του να χρησιμοποιείται στη διαδικασία του checksum. Είναι ένας απλός αριθμός που χρησιμοποιείται για την αναγνώριση συμβαλλόμενων μερών και διακατέχει μόνο αυτή τη σημασία. Είναι ένα μοναδικό αναγνωριστικό το οποίο δεν μπορεί να επαναχρησιμοποιηθεί.

3.6 Νέες Τεχνολογίες και Θέματα Νομοθεσίας

Η ραγδαία ανάπτυξη της τεχνολογίας με τις διάφορες τεχνολογικές δυνατότητες που προσφέρει, επιδρά με θετικό τρόπο στον επιστημονικό κόσμο. Ειδικότερα στην επιστήμη της ιατρικής, με τη χρήση πληροφοριακών συστημάτων σε ιατρικές εφαρμογές. Χάρη σε αυτή την εξέλιξη της τεχνολογίας, καινούριοι όροι όπως είναι το ηλεκτρονικό αρχείο υγείας και γενικότερα οι εφαρμογές ηλεκτρονικής υγείας, έχουν εμφανιστεί και έχουν κριθεί ως απαραίτητα συστατικά για τη βελτίωση των ιατρικών υπηρεσιών.

Το θέμα του ηλεκτρονικού αρχείου υγείας του ασθενή έχει εξεταστεί μέχρι τώρα κυρίως από την άποψη της προστασίας της επεξεργασίας των ιατρικών δεδομένων και την ελευθερία της διασυνοριακής διακίνησής τους.

Απαραίτητα συστατικά για τη δημιουργία ενός ΗΑΥ, είναι εργαλεία που προσφέρει η τεχνολογία όπως είναι οι βάσεις δεδομένων, οι ηλεκτρονικές υπογραφές, η χρήση του Διαδικτύου, οι έξυπνες κάρτες και γενικά μια μεγάλη πληθώρα εφαρμογών.

Η χρήση των εργαλείων της τεχνολογίας θα πρέπει να καλύπτεται από το νομοθετικό πλαίσιο. Μέχρι στιγμής στην Ευρωπαϊκή Ένωση, μέσω της νομοθεσίας, δίνονται γενικές κατευθυντήριες γραμμές για τη σωστή χρήση των τεχνολογιών, χωρίς να αναφέρονται πιο συγκεκριμένοι τεχνολογικοί τρόποι διασφάλισης της προστασίας των δεδομένων. Πιο κάτω παρουσιάζεται η νομοθεσία η οποία ισχύει στην Ευρωπαϊκή Ένωση και αφορά θέματα βάσεων δεδομένων, ηλεκτρονικών υπογραφών και έξυπνων καρτών.

3.6.1 Βάσεις Δεδομένων Υγείας

Μια βάση δεδομένων (database) υγείας είναι η συλλογή συσχετιζόμενων ιατρικών δεδομένων τα οποία είναι οργανωμένα με μεθοδικό τρόπο και στα οποία μπορεί κάποιος να έχει πρόσβαση με ηλεκτρονικά μέσα. Η χρήση των βάσεων δεδομένων έχει πολλά πλεονεκτήματα συμπεριλαμβανομένων και των πιο κάτω:

- Επιτρέπει την καλύτερη επεξεργασία των δεδομένων με ένα ενιαίο τρόπο.

- Επιτρέπει την καλύτερη οργάνωση και πρόσβαση στα ιατρικά αρχεία των ασθενών.
- Οι ιατρικές βάσεις αυξάνουν τη δυνατότητα λήψης αποφάσεων όλων όσων συμμετέχουν στο χώρο της υγείας.
- Τα δεδομένα τα οποία βρίσκονται στις βάσεις δεδομένων μπορούν να χρησιμοποιηθούν για έρευνα.
- Δεδομένου ότι υπάρχει ένα καλό σύστημα ασφαλείας για τη βάση δεδομένων, οι ηλεκτρονικοί φάκελοι υγείας, είναι πιο ασφαλείς από τα έγγραφα αρχεία, εφόσον οποιοσδήποτε μπορεί να κλέψει ένα έγγραφο αρχείο, χωρίς να αφήσει κάποιο ίχνος.

Με εμφάνιση του ηλεκτρονικού φακέλου ασθενή και με τη χρήση των βάσεων δεδομένων για την αποθήκευση της ιατρικής πληροφορίας, προκύπτει το θέμα της προστασίας των δεδομένων, ειδικά όταν αναφερόμαστε σε δεδομένα τα οποία ανήκουν στην κατηγορία των ευαίσθητων δεδομένων. Η αποθήκευση τέτοιων δεδομένων σε μια κεντρική θέση όπως είναι η βάση των δεδομένων, θέτει καινούργια ερωτήματα σχετικά με την προστασία των προσωπικών δεδομένων τα οποία δεν τίθενται όταν δεδομένα βρίσκονται στο χαρτί. Για παράδειγμα ποιος μπορεί να έχει πρόσβαση σε αυτά τα δεδομένα, πως χρησιμοποιείται η πληροφορία, πόσο ασφαλή είναι τα προσωπικά δεδομένα. Έτσι, έγκειται μεγάλη ανάγκη, η προστασία των προσωπικών δεδομένων να επικυρωθεί με την κατάλληλη νομοθεσία.

Πνευματική ιδιοκτησία ή πνευματικά δικαιώματα (copyright) ονομάζονται τα αποκλειστικά δικαιώματα των πνευματικών δημιουργών ενός έργου. Παραχωρούνται από τον νόμο και έχουν ισχύ για ένα ορισμένο χρόνο και απαγορεύουν σε τρίτους να χρησιμοποιούν τα έργα χωρίς την χρήση της συγκατάθεσης του δημιουργού του έργου. Το πνευματικό δικαίωμα αναφέρεται σε έργα λογοτεχνίας, τέχνης αλλά και άλλες δημιουργίες που αφορούν τεχνολογικά πεδία όπως λογισμικά συστήματα ή βάσεις δεδομένων. Περιλαμβάνει το δικαίωμα της εκμετάλλευσης του έργου (περιουσιακό δικαίωμα) και το δικαίωμα της προστασίας του προσωπικού δεσμού του δημιουργού του προς αυτό (ηθικό δικαίωμα). Το πνευματικό δικαίωμα αποτελεί ένα αυθαίρετο δικαίωμα του κάθε δημιουργού και ισχύει χωρίς να απαιτείται να γίνει αίτηση σε κάποιο φορέα είτε το έργο να αναγνωριστεί από κάποια υπηρεσία.

Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων: Η συγκεκριμένη οδηγία η οποία προέρχεται από το Ευρωπαϊκό Κοινοβούλιο, αναφέρεται στο πεδίο της προστασία δεδομένων οποιασδήποτε μορφής. Δηλαδή καλύπτει θέματα που αφορούν δεδομένα που βρίσκονται είτε σε ηλεκτρονική είτε σε συμβατική μορφή. Η οδηγία αυτή δεν περιέχει πρόνοιες που να αφορούν τα προγράμματα ηλεκτρονικών υπολογιστών που χρησιμοποιούνται για τη δημιουργία ή τη λειτουργία βάσεων δεδομένων, όπως είναι τα συστήματα διαχείρισης των βάσεων δεδομένων. Η νομική προστασία των λογισμικών προγραμμάτων που διαχειρίζονται βάσεις δεδομένων καλύπτονται μέσα από την οδηγία 91/250/EEC.

Σύμφωνα με το άρθρο 3, τα δεδομένα που περιέχονται σε μια βάση δεδομένων και ο τρόπος που είναι οργανωμένα, προστατεύονται σύμφωνα με το δικαίωμα του δημιουργού για το λόγο ότι αποτελούν πνευματικό του έργο. Δεν εφαρμόζονται κάποια άλλα κριτήρια εκτός από το δικαίωμα του δημιουργού έτσι ώστε να λαμβάνονται τα ανάλογα μέτρα προστασίας. Θα πρέπει να τονιστεί ότι η προστασία της βάσης δεδομένων σύμφωνα με το δικαίωμα του δημιουργού, δεν έχει ισχύ στο περιεχόμενο της βάσης και δεν αντιτάσσεται σε κανένα από τα δικαιώματα που υφίστανται για το συγκεκριμένο περιεχόμενο.

Για παράδειγμα, μια εταιρία η οποία αναλαμβάνει τη δημιουργία της βάσης ενός συστήματος ΗΑΥ, καθώς και το σχήμα της βάσης, θεωρείται ότι είναι ο δημιουργός της βάσης. Σύμφωνα με το νόμο αυτό, σε συνδυασμό με τη νομοθεσία για τη προστασία των προσωπικών δεδομένων, ο δημιουργός της βάσης δεν θα μπορεί να έχει πρόσβαση στο περιεχόμενο της βάση επικαλούμενος το δικαίωμα του δημιουργού.

Ο δημιουργός της βάσης των δεδομένων κατέχει το δικαίωμα να εκτελεί ή να επιτρέπει τις ακόλουθες πράξεις:

- Αναπαραγωγή της βάσης δεδομένων, είτε προσωρινά είτε σε ένα συνεχόμενο χρονικό διάστημα με οποιοδήποτε τρόπο και σε οποιαδήποτε μορφή. Αυτή η αναπαραγωγή μπορεί να είναι είτε τμηματική είτε να καλύπτει ολόκληρη τη βάση
- Δυνατότητα μετάφρασης, προσαρμογής και αλλαγής της διάταξης των στοιχείων που την απαρτίζουν ή οποιαδήποτε άλλη δυνατότητα μετατροπής καθώς και οποιαδήποτε δυνατότητα αναπαραγωγής, διανομής, ανακοίνωσης, παρουσίασης στο κοινό των αποτελεσμάτων των πράξεων αυτών.
- Ο δημιουργός της βάσης έχει το δικαίωμα να διανέμει είτε να αντιγράψει τη βάση δεδομένων του στο κοινό.

Είναι σημαντικό το γεγονός ότι επιτρέπεται η εκτέλεση οποιασδήποτε από τις πιο πάνω πράξεις από οποιοδήποτε νόμιμο χρήστη της βάσης. Ένας νόμιμος χρήστης μπορεί να εκτελέσει οποιαδήποτε διαδικασία χωρίς την άδεια του δημιουργού της βάσης στο βαθμό όπου του επιτρέπεται, ανάλογα με τα κατάλληλα δικαιώματα και εξουσιοδότηση που κατέχει.

3.6.2 Έξυπνες Κάρτες

Μια εφαρμογή της ηλεκτρονικής έξυπνης κάρτας στον χώρο της υγείας είναι η χρήση της ως ένα εργαλείο το οποίο θα αντικαταστήσει όλα τα έντυπα υγειονομικής περίθαλψης και ταυτόχρονα να διευκολύνει τους ασθενείς, τους φορείς παροχής υπηρεσιών περίθαλψης και τους οργανισμούς Κοινωνικής ασφάλισης. Αποτελεί ένα ηλεκτρονικό μητρώο υγείας, το οποίο μπορεί να αποτελεί τον αποθηκευτικό χώρο μιας σειράς από δεδομένα που αφορούν τον ασθενή.

Τέτοια στοιχεία μπορεί να περιλαμβάνουν κάποια σημαντικά χαρακτηριστικά τα οποία μπορούν να χρησιμοποιηθούν σε περιπτώσεις έκτακτης ανάγκης όπως είναι προσωπικά στοιχεία του ασθενή, άτομα για επικοινωνία σε περίπτωση ανάγκης, ιστορικό υγείας, αλλεργίες, ομάδα αίματος κλπ.

Ένα σημαντικό πρόβλημα για το υπάρχον υγειονομικό σύστημα είναι η πλαστογράφηση των ιατρικών δεδομένων. Η ηλεκτρονική έξυπνη κάρτα προσφέρει μέγιστη τεχνολογική ασφάλεια, εξασφαλίζοντας την ακεραιότητα, νομιμότητα και γνησιότητα της προέλευσης αυτών των δεδομένων.

Η προστασία προσωπικών δεδομένων του ασθενή διασφαλίζεται με την χρήση προσωπικού κωδικού (PIN). Μόνο με την εισαγωγή του κωδικού αυτού είναι δυνατή η ανάγνωση και η προσθήκη ιατρικών δεδομένων. Εκτός από την προστασία των προσωπικών δεδομένων του ασθενή, μπορεί να πιστοποιηθεί και η ταυτότητα του ιατρού ο οποίος μπορεί να προσπελάσει ή και να μεταβάλει τα ιατρικά δεδομένα του ασθενή. Αυτό επιτυγχάνεται και πάλι με τη χρήση επαγγελματική έξυπνης κάρτας αναγνώρισης του ιατρού ο οποίος χρησιμοποιεί προσωπικό κωδικό (PIN).

Οι έξυπνες κάρτες, λόγω της πρόσφατης εφαρμογής τους ως μέσο εκτέλεσης συναλλαγών αλλά και της πολυμορφίας ως προς τον τρόπο που μπορούν να χρησιμοποιηθούν και τα πεδία στα οποία μπορούν να εφαρμοστούν, δεν έχουν αποτελέσει στο παρόν στάδιο, αντικείμενο νομοθετικής ρύθμισης τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο.

Η καθιέρωσή τους είναι νεότευκτη και βρίσκεται σε πιλοτικό στάδιο ανάπτυξης σε συστήματα που αφορούν τη διακίνηση ιατρικών δεδομένων. Εμπόδιο στη χρήση τους αποτελεί η έλλειψη αυτούσιας νομοθεσίας που να αναφέρεται συγκεκριμένα σε αυτού του είδους την τεχνολογία. Σε επίπεδο ευρωπαϊκών οδηγιών, ελάχιστες είναι οι αναφορές στον όρο έξυπνη κάρτα και σε επίπεδο εθνικό είναι χαρακτηριστικό ότι αυτή η μορφή διακίνησης πληροφοριών δεν απαντάται σε καμία νομοθετική ρύθμιση.

Αναφορά στις έξυπνες κάρτες γίνεται σε πάρα πολλά κείμενα μη άμεσης υποχρεωτικής εφαρμογής τα οποία δεν αποτελούν μορφή νομοθεσίας όπως είναι ανακοινώσεις, στρατηγικές, συστάσεις, ψηφίσματα κλπ. Τέτοια κείμενα κυρίως προέκυψαν από ευρωπαϊκές στρατηγικές δράσης όπως είναι το eEurope2002 και eEurope2005 όπου φαίνεται ξεκάθαρα η θερμή υποστήριξη και πρόθεση να προωθηθεί η τεχνολογία των έξυπνων καρτών ως η βασική υποδομή η οποία θα αποδώσει λύσεις σε θέματα που αφορούν την ασφάλεια δεδομένων σε μια κοινωνία η οποία στηρίζεται στην πληροφορία.

3.6.3 Ηλεκτρονική Υπογραφή

Η ραγδαία ανάπτυξης της τεχνολογίας και του διαδικτύου και συνεπώς οι ηλεκτρονικές συναλλαγές μέσω των δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις διάφορες συναλλαγές. Ένας χρήστης του ΗΑΥ, απαιτεί τα δεδομένα τα οποία συμμετέχουν στις ηλεκτρονικές συναλλαγές να μην μπορούν να μεταποιηθούν κατά την μετάδοσή τους, να διατηρείται δηλαδή με αυτό τον τρόπο η εμπιστευτικότητα.

Επιπλέον, ο παραλήπτης των δεδομένων, πρέπει να είναι σίγουρος ότι αυτά που έχει παραλάβει χαρακτηρίζονται από ακεραιότητα και δεν διαφέρουν καθόλου από αυτά που έχει στείλει ο αποστολέας. Ακόμη, καθίσταται απαραίτητη προϋπόθεση ο παραλήπτης να γνωρίζει και να μην έχει καμία αμφιβολία για την αυθεντικότητα των δεδομένων και συνεπώς της ταυτότητας του αποστολέα. Ότι δηλαδή είναι ο πραγματικός αποστολέας και όχι κάποιος που προσποιείται τη ταυτότητά του. Όλοι οι εμπλεκόμενοι σε μια ηλεκτρονική συναλλαγή θα πρέπει να μην μπορούν να αποποιηθούν τη συμμετοχή τους στη συγκεκριμένη συναλλαγή.

Υπάρχουν διάφοροι μέθοδοι για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της αυθεντικότητας των δεδομένων. Η βαρύτητα για την ασφάλεια και προστασία των δεδομένων αυτών είναι μεγαλύτερη, όταν αυτά τα δεδομένα αποτελούν ευαίσθητα δεδομένα και ειδικά δεδομένα τα οποία έχουν σχέση με την υγεία του ατόμου. Θα πρέπει να αναπτυχθούν διάφορες τεχνικές για τη διασφάλιση των πιο πάνω ιδιοτήτων οι οποίες πάντα πρέπει να συνάδουν και να υπακούουν στην κατάλληλη νομοθεσία.

Η ιδιότητα της εμπιστευτικότητας των δεδομένων μπορεί να διασφαλιστεί με την κρυπτογραφία. Ο αποστολέας μπορεί να χρησιμοποιήσει μια μαθηματική συνάρτηση η οποία να μετατρέπει τα δεδομένα της συναλλαγής σε μια μορφή η οποία να μη μπορεί να διαβαστεί και να κατανοηθεί από οποιονδήποτε. Ο παραλήπτης, θα μπορεί να αποκρυπτογραφήσει τα δεδομένα και να τα φέρει στην κανονική τους μορφή γνωρίζοντας τον τρόπο.

Υπάρχουν διάφορες μέθοδοι για να πετύχουμε κρυπτογράφηση. Μια από τις μεθόδους ονομάζεται κρυπτογραφία δημοσίου κλειδιού όπου χρησιμοποιούνται δύο διαφορετικά κλειδιά. Ένα κλειδί για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση. Κάθε χρήστης έχει δύο κλειδιά. Το δημόσιο και το ιδιωτικό κλειδί. Το δημόσιο κλειδί είναι αυτό που μπορεί να γνωστοποιηθεί από τον χρήστη σε τρίτους. Το ιδιωτικό κλειδί είναι αυτό που αποθηκεύεται ασφαλή και μόνο ο συγκεκριμένος χρήστης το γνωρίζει και βρίσκεται στην κατοχή του. Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη. Έτσι, το μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη ο οποίος είναι ο μοναδικός κάτοχος του ιδιωτικού, αντίστοιχου κλειδιού εφόσον πάντα δεν έχει παραβιαστεί η ιδιωτικότητα του.

Για τη δημιουργία της ηλεκτρονικής υπογραφής χρησιμοποιείται η πιο πάνω μέθοδος. Ο χρήστης έχει στην κατοχή του τα δύο κλειδιά. Η σχέση των κλειδιών είναι τέτοια έτσι ώστε αν

κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφορά με τη κρυπτογράφηση, βρίσκεται στο γεγονός ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Η διαφορά με την ιδιόχειρη υπογραφή είναι ότι η ηλεκτρονική υπογραφή είναι διαφορετική για κάθε μήνυμα.

Για τη δημιουργία και ακολούθως την επαλήθευση της υπογραφής έχουμε την έννοια της συνάρτησης κατακερματισμού. Με την εφαρμογή αυτής της συνάρτηση, δημιουργείται μια σειρά από bits συγκεκριμένου μεγέθους από το μήνυμα, ανεξάρτητα από το μέγεθος του. Αυτή η συγκεκριμένη σειρά, αποτελεί μία ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για το μήνυμα το οποίο αντιπροσωπεύει.

Από τη σειρά που δημιουργείται, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σειρά από bits είναι πάρα πολύ μικρή. Έτσι ο παραλήπτης μπορεί εύκολα να διασφαλίσει την ακεραιότητα του μηνύματος που έχει παραλάβει εξετάζοντας αν το μήνυμα που έχει παραλάβει παράγει την ίδια σειρά από bits με εκείνη που του έχει αποσταλεί χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού.

Ο αποστολέας, έχοντας συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί την ταυτότητα του αποστολέα στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί του αποστολέα και συνεπώς πιστοποιεί την αυθεντικότητα. Έτσι η ταυτότητα του αποστολέα διασφαλίζεται μέσω των ιδιωτικών και δημοσίων κλειδιών που επαληθεύουν την υπογραφή του αποστολέα.

Για τη διασφάλιση της εμπιστευτικότητας, υπάρχει η ανάγκη ύπαρξης μιας έγκυρης τρίτης οντότητας, η οποία να πιστοποιεί την εγκυρότητα των ψηφιακών υπογραφών. Αυτή η οντότητα είναι η υπηρεσία παροχής πιστοποίησης. Ο αποστολέας και ο παραλήπτης αποκτούν τα κλειδιά που χρειάζονται για την κρυπτογράφηση και επαλήθευση της ηλεκτρονικής υπογραφής από Παροχείς Υπηρεσιών Πιστοποίησης. Η υπηρεσία αυτή, είναι υπεύθυνη για την έκδοση ψηφιακών πιστοποιητικών τα οποία περιέχουν στοιχεία ταυτοποίησης όπως για παράδειγμα το όνομα και το επίθετο των κατόχων των συγκεκριμένων κρυπτογραφικών κλειδιών. Επιπλέον, περιέχει και κάποια άλλα πεδία όπως είναι ο σειριακός αριθμός πιστοποιητικού, ημερομηνία έκδοση και λήξης και στοιχεία του εκδότη.

Η ηλεκτρονική υπογραφή, αποτελεί ένα σημαντικό παράγοντα για τη δημιουργία ενός πετυχημένου συστήματος ηλεκτρονικού φακέλου, εφόσον θα μπορεί να διασφαλίζει την εμπιστευτικότητα και την αυθεντικότητα της διακίνησης ιατρικών δεδομένων μέσω ενός δικτύου.

Για να μπορεί να υλοποιηθεί η ηλεκτρονική υπογραφή, θα πρέπει να υπάρχει η κατάλληλη νομοθεσία έτσι ώστε να καθιστά τη χρήση της δυνατή.

Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές: Ο σκοπός αυτής της οδηγίας είναι η διευκόλυνση της χρήσης των ηλεκτρονικών υπογραφών έτσι ώστε να γίνουν και νομικά αποδεκτές. Θεσπίζει ένα νομικό πλαίσιο τόσο για τις ηλεκτρονικές υπογραφές όσο και για ορισμένες υπηρεσίες πιστοποίησης.

Τα κράτη μέλη της Ευρωπαϊκής Ένωσης, διασφαλίζουν ότι ηλεκτρονικές υπογραφές που βασίζονται σε κάποιο αναγνωρισμένο πιστοποιητικό και δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής, μπορούν να χρησιμοποιηθούν ως αποδεικτικό στοιχείο σε νομικές διαδικασίες. Επιπλέον, όπως μια ιδιόχειρη υπογραφή ικανοποιεί τις νομικές απαιτήσεις σε σχέση με δεδομένα που βρίσκονται αναγραμμένα στο χαρτί, έτσι και οι ηλεκτρονικές υπογραφές θα πρέπει να ικανοποιούν τις αντίστοιχες νομικές απαιτήσεις για τα ηλεκτρονικά δεδομένα.

Τα κράτη εξασφαλίζουν ότι οι παροχείς υπηρεσιών πιστοποίησης και οι εθνικοί φορείς, αρμόδιοι για πιστοποίηση ή εποπτεία, ακολουθούν και υπακούουν τις απαιτήσεις που καθορίζονται στην οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των ατόμων σχετικά με την επεξεργασία και την ελεύθερη διακίνηση των προσωπικών δεδομένων. Επίσης εξασφαλίζουν ότι ένας παροχέας ο οποίος εκδίδει πιστοποιητικά, θα πρέπει να διασφαλίζει τα προσωπικά δεδομένα που χρειάζεται μόνο από το άτομο στο οποίο αναφέρονται τα δεδομένα ή διασφαλίζοντας τη συγκατάθεσή του, στο επίπεδο πάντα όπου είναι απαραίτητο. Επίσης οι παροχείς μπορούν να χρησιμοποιήσουν ψευδώνυμο αντί το όνομα του ατόμου που υπογράφει, έχοντας υπόψη τις συνέπειες της εθνικής νομοθεσίας.

Η οδηγία αυτή δεν έχει ως σκοπό την εναρμόνιση των εθνικών νόμων που περιλαμβάνουν τις ανάλογες κυρώσεις σε περιπτώσεις παραβίασης του δικαίου. Έτσι, οι διατάξεις που αφορούν τις συνέπειες του νόμου σχετικά με τις ηλεκτρονικές υπογραφές, θα πρέπει να ακολουθούν την εθνική νομοθεσία.

Η οδηγία ορίζει ότι πιστοποιητικά μπορούν να χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας του προσώπου που υπογράφει ηλεκτρονικά. Με τον τρόπο αυτό, οι ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό έχουν σαν στόχο, ένα πιο υψηλό επίπεδο ασφάλειας και εφόσον έχουν δημιουργηθεί από ασφαλή διάταξη δημιουργίας υπογραφής, μπορούν να θεωρηθούν νομικά ισοδύναμες με τις ιδιόχειρες υπογραφές μόνον εφόσον πληρούνται οι εν λόγω προϋποθέσεις για τις ιδιόχειρες υπογραφές.

3.7 Συμπεράσματα

Όπως και σε οποιοδήποτε πληροφοριακό σύστημα, η ασφάλεια του ΠΣΥ είναι ένας κρίσιμος παράγοντας. Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα είναι ιδιότητες της ασφαλείας των δεδομένων. Η επιτυχία ενός συστήματος ΗΑΥ του ασθενή και συνεπώς η αποδοχή του από τους χρήστες και ιδιαίτερα από τους ασθενείς, εξαρτάται σε μεγάλο βαθμό από το υψηλό επίπεδο ασφάλειας των δεδομένων που θα παρέχει. Η πρόσβαση μη εξουσιοδοτημένων ατόμων θα πρέπει να είναι αδύνατη και να αποτρέπεται με κάθε δυνατό τρόπο. Εν αντιθέσει, η πρόσβαση σε εξουσιοδοτημένους επαγγελματίες υγείας, ειδικά σε περιπτώσεις έκτακτης ανάγκης, δεν πρέπει να είναι υπό όρους στα πλαίσια της ιατρικής περίθαλψης, εφόσον κύριος σκοπός του συστήματος είναι η παροχή ποιοτικών υπηρεσιών ιατρικής περίθαλψης.

Η ασφάλεια των ΠΣΥ, μπορεί να εφαρμοστεί με τη φυσική ασφάλεια του συστήματος, η οποία παρέχει πρόσβαση μόνο στους εξουσιοδοτημένους χρήστες, μέσω της εφαρμογής τεχνολογιών αναχώματος, κρυπτογράφησης και ανταλλαγής δεδομένων πάνω από ασφαλή κανάλια επικοινωνίας.

Ευαίσθητες πληροφορίες υγείας, όπως πληροφορίες για τον ιό HIV, την ψυχική κατάσταση του ασθενή, θα μπορούσαν να γίνουν πιο εύκολα προσιτές καθώς τα αρχεία ασθενών ωθούνται προς την πλήρη αυτοματοποίηση. Εάν οι ευαίσθητες πληροφορίες υγείας είναι προσβάσιμες από τρίτους, αυτό θα αντιπροσώπευε την παραβίαση της ιδιωτικότητας του ασθενή.

Οι παροχείς υπηρεσιών υγείας και άλλοι συμμετέχοντες, έχουν το καθήκον να διατηρήσουν την εμπιστευτικότητα των δεδομένων και των συστημάτων, και να αποτρέψουν την πρόσβαση σε χρήστες οι οποίοι δεν έχουν τα κατάλληλα δικαιώματα πρόσβασης. Επομένως, το νομοθετικό πλαίσιο το οποίο θα πρέπει να θεσπιστεί για τη νομική κάλυψη αυτού του εγχειρήματος, θα πρέπει να προβλέπει την εφαρμογή των κατάλληλων μέτρων ασφαλείας, τόσο τεχνικών όσο και οργανωτικών, με στόχο την αποτροπή της ανάγνωσης, επεξεργασίας και τροποποίησης των δεδομένων από μη εξουσιοδοτημένα άτομα καθώς και της οποιασδήποτε μορφής απώλειας.

Με την ραγδαία ανάπτυξη της τεχνολογίας δημιουργείται συνεχώς μεγαλύτερη ανάγκη για προστασία των προσωπικών δεδομένων και δικαιωμάτων των ασθενών. Επομένως, αναμένονται συνεχείς δραστηριότητες βελτίωσης της προστασίας των δεδομένων ανάλογα με τις ανάγκες που προκύπτουν. Η νομοθεσία θα πρέπει να εκτιμά τους κινδύνους σχετικά με την ασφάλεια των προσωπικών δεδομένων, πριν την υλοποίηση του συστήματος, διασφαλίζοντας έτσι τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία ανήκουν τα δεδομένα.

Κεφάλαιο 4

Ζητήματα Ασφάλειας σε Πληροφοριακά Συστήματα Υγείας

4.1 Εισαγωγή

Η ασφάλεια ΠΣΥ θεωρείται ως κρίσιμο ζήτημα από την αρχή της υλοποίησής τους, ιδίως για το γεγονός ότι τα δεδομένα τους θεωρούνται ότι αποτελούν εξαιρετικά ευαίσθητες πληροφορίες. Η ικανότητα αποθήκευσης πληροφοριών υγείας σε ηλεκτρονική μορφή εγείρει ανησυχίες σχετικά με την ιδιωτικότητα των ασθενών και την ασφάλεια των δεδομένων. Ως εκ τούτου, σε οποιαδήποτε προσπάθεια εισαγωγής ηλεκτρονικών ΠΣΥ θα πρέπει να διασφαλίζεται η επαρκής προστασία της εμπιστευτικότητας και της ακεραιότητας των πληροφοριών του ασθενή. Ταυτόχρονα, οι πληροφορίες του ασθενή πρέπει να είναι άμεσα διαθέσιμες σε όλους τους εξουσιοδοτημένους παρόχους υγειονομικής περίθαλψης, προκειμένου να εξασφαλιστεί η κατάλληλη θεραπεία του ασθενή.

Παρόλα αυτά, η αυξανόμενη διαθεσιμότητα των πληροφοριών των ασθενών αυξάνει και τις απειλές ενάντια της ασφάλειας. Προκειμένου να απλοποιηθεί η πολυπλοκότητα του χώρου, αλλά και ταυτόχρονα να προστατεύεται η ασφάλεια και η ιδιωτικότητα σε ΠΣΥ, θα πρέπει να εφαρμοστούν κατάλληλες υπηρεσίες και μηχανισμοί ασφάλειας. Στο κεφάλαιο αυτό παρουσιάζεται μια επισκόπηση των υφιστάμενων τάσεων όσον αφορά τις πτυχές της ασφάλειας των ΠΣΥ.

4.2 Νέες Τεχνολογίες και Ζητήματα Ασφάλειας

Τα ΠΣΥ απαρτίζονται από διάφορες τεχνολογίες οι οποίες ελέγχουν, ενημερώνουν και αποφασίζουν όσον αφορά την φροντίδα του ασθενή. Αυτές οι τεχνολογίες επιτρέπουν στον ασθενή να πράττει ενεργά στην προσωπική του φροντίδα. Συνεπώς, οι τεχνολογίες αυτές συνεισφέρουν στην βελτίωση της ποιότητας της φροντίδας, ενώ ταυτόχρονα μειώνουν τυχόν ανεπιθύμητο κόστος και ιατρικά λάθη. Οι τεχνολογίες παρέχουν ποικίλα οφέλη στον τομέα της υγείας. Παρόλα αυτά, προκύπτουν διάφορα ζητήματα ασφάλειας και ιδιωτικότητας που πρέπει να αντιμετωπιστούν προκειμένου να εκμεταλλευτούμε στο έπακρο τα πλεονεκτήματα από την εφαρμογή τους. Τα ζητήματα αυτά περιλαμβάνουν (Meingast, Roosta, and Sastry, 2007):

- Ασφάλεια δεδομένων κατά την μεταφορά τους
- Ασφάλεια δεδομένων κατά την αποθήκευσή τους

- Ποσότητα των αποθηκευμένων δεδομένων
- Δικαιώματα ανάλυσης δεδομένων
- Πολιτικές και κανονισμοί ελέγχου
- Υπευθυνότητα
- Μη αποποίηση

4.2.1 Ηλεκτρονικό Αρχείο Υγείας

Στο παρελθόν, τα αρχεία υγείας των ασθενών φυλάσσονταν σε χειρόγραφη μορφή και ήταν αποθηκευμένα σε αποθήκες αρχείων στο εσωτερικό των οργανισμών υγείας. Η χρήση των ΗΑΥ μετατρέπει τα χειρόγραφα αρχεία σε ψηφιακές αναπαραστάσεις στις οποίες η πρόσβαση γίνεται ηλεκτρονικά. Τα ΗΑΥ πιθανόν πλέον να αποθηκεύονται σε βάσεις δεδομένων εκτός οργανισμού.

Η χρήση των ΗΑΥ βοηθά στην αποφυγή λαθών και παρεξηγήσεων αναγνωσιμότητας, μειώνοντας ταυτόχρονα το κόστος λειτουργίας και βελτιώνοντας την φροντίδα του ασθενή. Στις ΗΠΑ, ο θάνατος 7000 ασθενών ετησίως, οφείλεται σε λάθη συνταγογράφησης που κοστίζουν περισσότερο από 6 δισεκατομμύρια δολάρια (Kingsbury, 2008).

Τα ΗΑΥ είναι η βάση των ΠΣΥ τα οποία εξαρτώνται από την έγκαιρη πρόσβαση στις ιατρικές πληροφορίες των ασθενών. Το περιεχόμενο των ΗΑΥ ποικίλει από οργανισμό σε οργανισμό, αλλά γενικά τα ΗΑΥ περιέχουν προσωπικά δεδομένα που σχετίζονται με την συνταγογράφηση, τωρινή νοητική και φυσική υγεία, αναφορές διαγνώσεων κτλ. Σε συστήματα ΗΑΥ διεθνώς, οι πληροφορίες εκατομμυρίων ασθενών ψηφιοποιούνται για περεταίρω αποθήκευση, επεξεργασία και μεταβίβαση. Όμως, εγείρονται ανησυχίες για την ασφάλεια και ιδιωτικότητα εξαιτίας της έκτασης και της ευκολίας διάδοσης πληροφοριών υγείας. Επιπλέον, ο αυξανόμενος αριθμός των ατόμων που επιθυμούν την πρόσβαση σε αυτές τις πληροφορίες, οξύνει το πρόβλημα. Η αποκάλυψη των ΗΑΥ μπορεί να έχει καταστροφικές συνέπειες για τον ασθενή. Τα ζητήματα ασφάλειας και ιδιωτικότητας θεωρούνται ως ο πιο ανασταλτικός παράγοντας για την αποδοχή και εφαρμογή τέτοιων συστημάτων (Ray and Wimalasiri, 2006). Επαρκή μέτρα ασφάλειας δεν λαμβάνονται κατά την αποθήκευση, επεξεργασία και μεταφορά ΗΑΥ. Η έλλειψη αυστηρών μέτρων ελέγχου πρόσβασης θα μπορούσε να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες ιατρικές πληροφορίες.

Τα ΗΑΥ αποτελούν μια σημαντική εξέλιξη της τεχνολογίας και παρέχουν στους ασθενείς την ευκαιρία να αποκομίσουν εξαιρετικά οφέλη από την κλινική φροντίδα, την έρευνα και την παροχή υγειονομικής περίθαλψης. Παρόλα αυτά, τα ΗΑΥ είναι σε θέση να παρέχουν αυτά τα οφέλη με την προϋπόθεση ότι εξασφαλίζεται η ιδιωτικότητα και η εμπιστευτικότητα του ασθενή.

4.2.2 Μεταφορά Ιατρικής Πληροφορίας μέσω Διαδικτύου και Προτεινόμενες Λύσεις

Το Διαδίκτυο χρησιμοποιείται σε μια πληθώρα δραστηριοτήτων συμπεριλαμβανομένου και της μεταφοράς ιατρικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου. Τα οφέλη της αυξημένης πρόσβασης σε ιατρικές πληροφορίες, όμως, έχουν δημιουργήσει διλήμματα. Κρίσιμο ζήτημα θεωρείται η απόκτηση, χρήση και ανταλλαγή πληροφοριών για την παροχή φροντίδας, χωρίς ταυτόχρονα να παραβιάζεται η ιδιωτικότητα του ασθενή. Ακόμη ένα πρόβλημα που αντιμετωπίζεται στον τομέα της υγείας είναι η διαθεσιμότητα ακριβών και ενημερωμένων πληροφοριών. Φυσικά, υπάρχουν τεχνικές λύσεις που έχουν προταθεί και που συνεισφέρουν στην βελτίωση της ασφάλειας και ιδιωτικότητας, σε ένα περιβάλλον πολλών χρηστών.

Κρυπτογραφία: Η κρυπτογραφία είναι η κύρια τεχνολογία με την οποία αποτρέπονται τρίτα μέλη να διαβάσουν εμπιστευτικές πληροφορίες ασθενών. Με την εφαρμογή της κρυπτογραφίας, τα δεδομένα υγείας μετατρέπονται με τέτοιο τρόπο ώστε οποιοσδήποτε ανακτήσει τα δεδομένα, να μην αντιλαμβάνεται το περιεχόμενο. Μόνο εξουσιοδοτημένοι χρήστες μπορούν να μετατρέψουν τα δεδομένα στην αρχική τους μορφή. Επιπλέον, η κρυπτογραφία αποτρέπει την παρακολούθηση και εφαρμόζεται σε υλικό καθώς και λογισμικό. Προκειμένου να εξασφαλιστεί το βέλτιστο επίπεδο ασφάλειας, προτείνεται να χρησιμοποιούνται και οι δυο προσεγγίσεις κρυπτογραφίας, δηλαδή η συμμετρική και η ασύμμετρη. Διάφορα κλειδιά ασύμμετρων και συμμετρικών αλγορίθμων μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση λογισμικού.

Μηχανισμοί αυθεντικοποίησης: Οι μηχανισμοί αυθεντικοποίησης χρησιμοποιούνται για να εξασφαλιστεί ότι ο άνθρωπος/οντότητα που στέλνει τα δεδομένα, είναι αυτός που ισχυρίζεται. Έχει αναπτυχθεί μια πληθώρα αλγορίθμων αυθεντικοποίησης όπως κωδικοί πρόσβασης, ψηφιακές υπογραφές, βιομετρικές συσκευές, αναχώματα και πρωτόκολλα αυθεντικοποίησης. Η χρήση όμως του Διαδικτύου, αυξάνει τις απειλές της μη εξουσιοδοτημένης πρόσβασης. Υπάρχουν μέθοδοι που έχουν σχεδιαστεί όπως το PCASSO (Patient Centered Access to Secure Systems Online), που βασικός στόχος του είναι να επιτρέπει σε παρόχους υγειονομικής περίθαλψης καθώς και σε καταναλωτές, να έχουν ασφαλή πρόσβαση σε ιατρικές πληροφορίες, συμπεριλαμβανομένου και των ευαίσθητων κλινικών δεδομένων, μέσω του Διαδικτύου.

4.2.3 Μηχανισμοί Ελέγχου Πρόσβασης

Οι μηχανισμοί ελέγχου πρόσβασης είναι απαραίτητοι για την προστασία των ευαίσθητων πληροφοριών του ασθενή. Αυτοί οι μηχανισμοί πρέπει να παρέχουν ταυτόχρονη πρόσβαση σε διαφορετικά δεδομένα του ασθενή όπως, για παράδειγμα, ιστορικό υγείας, κλινική περίπτωση ασθενή, διοικητικά δεδομένα κτλ. Επιπλέον, οι ασθενείς αποκτούν πρόσβαση σε διάφορες υπηρεσίες και λειτουργίες του νοσοκομείου που βελτιώνουν την άνεση και την ασφάλειά τους. Η

απομακρυσμένη παρακολούθηση της κατάστασης της υγείας του ασθενούς γίνεται όλο και πιο σημαντική με την εξέλιξη της εποπτείας του ασθενούς.

Ο έλεγχος πρόσβασης περιλαμβάνει δύο κύριες πτυχές. Αφενός, να απορρίπτεται η πρόσβαση σε ιατρικά δεδομένα σε χρήστες οι οποίοι δεν έχουν δικαίωμα πρόσβασης, και αφετέρου, να εξασφαλίζεται η πρόσβαση σε όλα τα σχετικά δεδομένα, σε όλους τους χρήστες των βάσεων δεδομένων που ασκούν το δικαίωμα πρόσβασης τους με συμβατικό τρόπο. Η αποτελεσματικότητα των μηχανισμών ελέγχου πρόσβασης γενικά εξαρτάται από τρεις βασικές υποθέσεις:

- Την σωστή ταυτοποίηση του χρήστη
- Την παρεμπόδιση απροσδόκητων παρατηρητών να αποκτήσουν πρόσβαση σε τμήματα της βάσης δεδομένων
- Την κατάλληλη προστασία των προνομιακών πληροφοριών.

Συνεπώς, κύριος στόχος είναι η ανάπτυξη και η εφαρμογή μηχανισμών ελέγχου πρόσβασης που θα προστατεύουν τα ιατρικά δεδομένα των ασθενών. Όσον αφορά τους μηχανισμούς αυτούς, ο χρήστης θα επιτρέπεται να έχει πρόσβαση μόνο σε πληροφορίες απαραίτητες για την ολοκλήρωση της εργασίας του. Για παράδειγμα, μια γραμματέας δεν θα είναι σε θέση να αποκτήσει πρόσβαση στα κλινικά δεδομένα ενός ασθενή, σε αντίθεση με έναν γιατρό. Ο έλεγχος πρόσβασης βασισμένος σε ρόλους (Role Based Access Control-RBAC), είναι το κυρίαρχο μοντέλο για προηγμένο έλεγχο πρόσβασης. Το μοντέλο RBAC υποστηρίζει αρχές της ασφάλειας όπως αυτή των ελάχιστων δικαιωμάτων, και επιπλέον, οδηγεί στη μείωση της πολυπλοκότητας και του κόστους της διαχείρισης της ασφάλειας σε συστήματα ευρείας κλίμακας.

Παρόλα αυτά, το μοντέλο RBAC θεωρείται ότι είναι ανεπαρκές για να ικανοποιήσει πλήρως τις απαιτήσεις ελέγχου πρόσβασης σε περιβάλλοντα υγείας (Hu and Weaver, 2004). Αυτό επειδή δεν λαμβάνει υπόψη το πλαίσιο ενεργοποίησης-απενεργοποίησης των δικαιωμάτων πρόσβασης. Συγκεκριμένα, αν ένας γιατρός απουσιάζει δεν υπάρχει τρόπος με τον οποίο κάποιος άλλος γιατρός θα μπορούσε να αναλάβει τα προνόμια επί των πόρων του σε περίπτωση έκτατης ανάγκης. Συνεπώς, δεν έχει δημιουργηθεί ακόμη κάποιο μοντέλο που μπορεί να θεωρηθεί ως το πλέον κατάλληλο για ΠΣΥ.

4.2.4 Ασφάλεια Βάσεων Δεδομένων

Η έννοια της ασφάλειας των Βάσεων Δεδομένων (ΒΔ) αναφέρεται στην ικανότητα ενός συστήματος να επιβάλει πολιτικές ασφάλειας που διέπουν την κοινοποίηση, τροποποίηση ή την καταστροφή πληροφοριών. Ένα από τα πλεονεκτήματα των υφιστάμενων ΒΔ είναι η ικανότητά τους να επιβάλλουν περιορισμούς ακεραιότητας σε παγκόσμια κλίμακα, σε ένα μεγάλο κομμάτι

δεδομένων. Η είσοδος αντιφατικών δεδομένων απορρίπτεται από τα εν λόγω συστήματα, προκειμένου να διατηρηθεί η ορθότητα. Από την άλλη πλευρά, στα ΠΣΥ, μπορεί να είναι αναγκαίο να υλοποιηθούν δύο ή περισσότερες ΒΔ σε ένα σύστημα. Για παράδειγμα, αν ένας γιατρός επιθυμεί να κρύψει το πραγματικό όνομα μιας πιθανής ασθένειας από έναν ασθενή σε κρίσιμη κατάσταση, μέχρις ότου η διάγνωση έχει επιβεβαιωθεί από εργαστηριακές εξετάσεις, η ΒΔ που προβάλλεται στον ασθενή θα πρέπει να είναι διαφορετική από εκείνη που χρησιμοποιεί ο γιατρός. Παρόλα αυτά, καταστάσεις σαν και αυτή πρέπει νε είναι ελεγχόμενες καθώς οι διαφορετικές αυτές ΒΔ, πρέπει να είναι σε θέση να ανταλλάσουν δεδομένα. Οι βασικοί στόχοι της ασφάλειας των ιατρικών ΒΔ είναι να υποστηρίζεται ένα υψηλό επίπεδο διαθεσιμότητας, ακρίβειας και συνάφειας των αποθηκευμένων δεδομένων των ασθενών, προκειμένου να παρέχεται το ιατρικό απόρρητο και η εμπιστευτικότητα και να προστατεύεται η ιδιωτικότητα του ασθενή.

Οι απαιτήσεις ασφάλειας για ιατρικές ΒΔ μπορούν να ταξινομηθούν ως εξής:

- Υλοποίηση πολιτικών εξουσιοδότησης που προσδιορίζουν το ποιος έχει πρόσβαση και σε τι είδος πληροφορίες του ασθενή. Ο κύριος στόχος τους είναι να παρέχεται ένα επαρκές επίπεδο μυστικότητας ενώ ταυτόχρονα να διατηρείται η ακεραιότητα.
- Η συνάφεια και η ορθότητα των δεδομένων στην ΒΔ αποτελούν βασικές απαιτήσεις. Ανακριβή δεδομένα μπορεί να έχουν καταστροφικές συνέπειες, όπως η λανθασμένη διάγνωση ενός ασθενή.
- Πολιτικές για την διαθεσιμότητα δεδομένων είναι απαραίτητες. Για παράδειγμα, ο γιατρός μιας βάρδιας μπορεί να χρειαστεί να έχει πρόσβαση στις πληροφορίες ενός ασθενή, σε περίπτωση εκτάκτου ανάγκης, προκειμένου να είναι σε θέση να λάβει μέτρα για την θεραπεία του γρήγορα και αποτελεσματικά.
- Οι πολιτικές ελέγχου πρέπει να είναι αρκετά λεπτομερείς ώστε να είναι χρήσιμες.

Προς το παρόν, οι τάσεις που διακρίνονται ανάμεσα σε διάφορες προτάσεις σχετικά με τις ιατρικές πολιτικές ασφάλειας των ΒΔ, και περιγράφουν τις απαιτήσεις εξουσιοδότησης σε ένα σύστημα ΒΔ είναι οι εξής:

- Υποχρεωτική ή πολλαπλών επιπέδων πολιτική ασφάλειας ιατρικών ΒΔ: Η ανάγκη για μια πολιτική ασφάλειας πολλαπλών επιπέδων προκύπτει όταν ένα ιατρικό σύστημα ΒΔ περιέχει πληροφορίες με ποικίλες ταξινομήσεις ασφάλειας, όπως απλά δεδομένα, απόρρητα και ευαίσθητα. Αυτή η πολιτική ασφάλειας περιορίζει την πρόσβαση σε απόρρητες πληροφορίες και σε εξουσιοδοτημένους χρήστες. Συγκεκριμένα, απαιτεί τα απόρρητα δεδομένα να προστατεύονται όχι μόνο από την άμεση πρόσβαση μη εξουσιοδοτημένων χρηστών, αλλά και από την αποκάλυψή τους με έμμεσους τρόπους.

- Προαιρετική πολιτική ασφάλειας ιατρικών ΒΔ: Ο προαιρετικός έλεγχος πρόσβασης έχει σχεδιαστεί κατά τρόπο ώστε να επιβάλλει μια συγκεκριμένη πολιτική ελέγχου πρόσβασης, η οποία χρησιμοποιείται για να καθορίσει τους κανόνες βάσει των οποίων οι χρήστες μιας ιατρικής ΒΔ μπορούν να ζητήσουν πρόσβαση σε αυτήν. Οι μηχανισμοί αυτοί βασίζονται συνήθως σε κάποιο είδος λίστας ελέγχου πρόσβασης (access control lists), που προσδιορίζουν σε ποιον επιτρέπεται η πρόσβαση και σε τι είδος πληροφορίες. Επίσης, οι προαιρετικές πολιτικές ασφάλειας ρυθμίζουν και θέματα που αφορούν την χορήγηση, ανάκληση και απόρριψη εξουσιοδότησης από και προς τους χρήστες.
- Πολιτική ασφάλειας ΒΔ βασισμένη στην προσωπική γνώση: Κύριος σκοπός της παρούσας πολιτικής είναι η στήριξη της ιδιωτικότητας των δεδομένων του ασθενούς πάνω από οποιοδήποτε άλλο στόχο σχεδιασμού. Η προσέγγιση αυτή, επιδιώκει να συνδέσει την γνώση (πληροφορίες ασθενών) με παράγοντες που πρέπει να διαθέτουν αυτήν (γιατρούς) και εν συνεχεία, να χαρτογραφήσουν την αντίληψη αυτή της γνώσης σε κατάλληλες έννοιες προγραμματισμού.

Κανένας από τους μηχανισμούς που παρουσιάζονται μέχρι σήμερα δεν αποτελεί την βέλτιστη λύση, εντούτοις, είναι δυνατόν νε επιτευχθεί ένα αποδεκτό επίπεδο ασφάλειας συνδυάζοντας δύο ή περισσότερες από τις παραπάνω μεθόδους. Όλα τα λειτουργικά ΠΣΥ περνούν από μια συνεχή εξελικτική διαδικασία. Αυτή η εξέλιξη, θα πρέπει επομένως, να θεωρείται αναμενόμενη και κατά τον σχεδιασμό μιας ασφαλούς ιατρικής ΒΔ.

4.3 Ανάλυση και Διαχείριση Κινδύνου σε ΠΣΥ

Στον τομέα της υγείας, ακόμη και μια ελάχιστη απώλεια πληροφοριών μπορεί να οδηγήσει στην απώλεια ανθρώπινης ζωής. Ως κίνδυνος-ρίσκο για την ασφάλεια, ορίζεται, η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια του συστήματος. Ο κίνδυνος θεωρείται επίσης ότι απαρτίζεται από τις τρεις ακόλουθες συνιστώσες:

- Απειλή: Ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, τυχαία ή με πρόθεση μετατροπή των δεδομένων, καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών. Μια χαρακτηριστική απειλή ενός ΠΣΥ είναι η απόκτηση μη εξουσιοδοτημένης πρόσβασης σε αρχεία ασθενών, ή η διακοπή τροφοδοσίας ρεύματος που ενδέχεται να εμποδίσει την διαθεσιμότητα των κλινικών δεδομένων του ασθενή.
- Ευπάθεια: Μια αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, εφαρμογή ή υποδομή που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος.

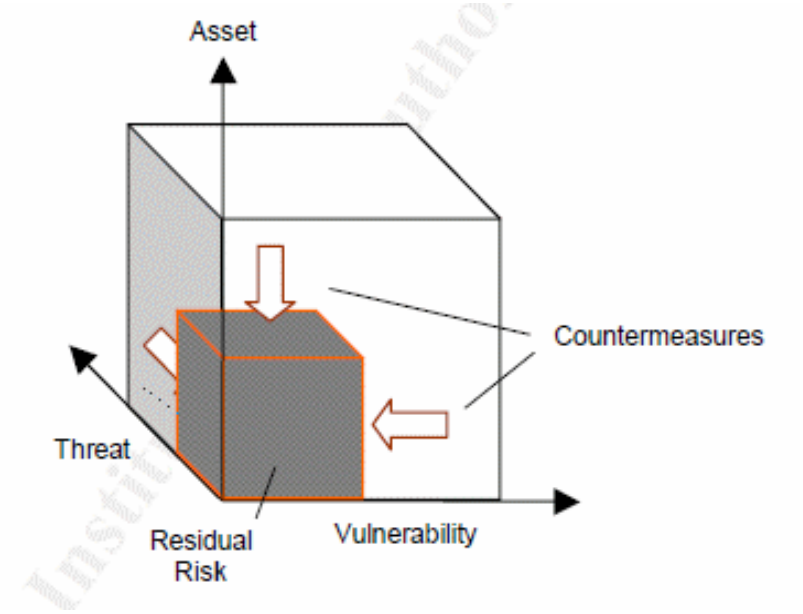
- Συνέπεια: Οι συνέπειες που θα μπορούσαν να προκύψουν σε μια μονάδα υγείας, αν τελικά η εμφάνιση μιας απειλής εκμεταλλευτεί μια ευπάθεια και επηρεάσει δυσμενώς ένα ή περισσότερα περιουσιακά στοιχεία-πόρους από τα οποία αποτελείται το σύστημα. Θα πρέπει στο σημείο αυτό να αναφερθεί ότι με τον όρο «περιουσιακά στοιχεία» δεν εννοούνται μόνο τα καθαρά οικονομικά μεγέθη. Αντιθέτως, συμπεριλαμβάνονται και αξίες όπως προσωπικά δεδομένα, στοιχεία που η παραβίαση τους μπορεί να οδηγήσει στην απώλεια ανθρώπινης ζωής, η εικόνα ενός οργανισμού προς τα έξω κτλ.

Επιπλέον, το ρίσκο, η πιθανότητα πρόκλησης ζημιάς ή απώλειας, περιγράφεται ως επί το πλείστον συναρτήσει της απειλής και της ευπάθειας ή της συνέπειας και της πιθανότητας. Το γενικό πλαίσιο που παρατίθενται στο [CRA98] του 1992 NIST, επισημοποιεί έξι στοιχεία του ρίσκου:

- Περιουσιακά στοιχεία-Πόροι
- Ευπάθειες
- Απειλές
- Συνέπειες
- Πιθανότητες
- Μέτρα προστασίας

Με τα δεδομένα αυτά υπολογίζεται το ρίσκο που εισάγει η χρήση κάθε πληροφοριακού συστήματος στην λειτουργία του οργανισμού. Έτσι, μπορούν να υπολογιστούν με ικανοποιητική ακρίβεια ποια αντίμετρα συμφέρει να εγκατασταθούν και σε ποιες περιπτώσεις είναι προτιμότερη η αποδοχή του ρίσκου. Εν ολίγης, ο υπολογισμός του ρίσκου μπορεί να καθοριστεί ως προϊόν των απειλών, των ευπαθειών και της αξίας των περιουσιακών στοιχείων:

Ρίσκο = περιουσιακό στοιχείο * απειλή * ευπάθεια



Σχήμα 4.1 *Ρίσκο ως συνάρτηση της αξίας του περιουσιακού στοιχείου, της απειλής και της ευπάθειας*

Τα στοιχεία του ρίσκου και τα ανάλογα αντίμετρά του μπορούν να απεικονιστούν καλύτερα με έναν κύβο (Σχήμα 4.1). Το σύστημα χαρακτηρίζεται από ένα αρχικό επίπεδο ρίσκου πριν εφαρμοστεί σε αυτό κάποιο από τα αντίμετρα. Τα αντίμετρα, υποθέτοντας ότι οι τιμές τους αποδίδονται σύμφωνα με τις ίδιες παραμέτρους που χρησιμοποιούνται για την απειλή, την ευπάθεια και την αποτίμηση περιουσιακών στοιχείων, μπορούν να μειώσουν τον κίνδυνο με την μείωση απειλών (πχ αναχώματα), την μείωση ευπαθειών (πχ ενημέρωση, patches) ή την μείωση της αξίας των περιουσιακών στοιχείων (πχ κρυπτογράφηση). Μετά τον υπολογισμό των αποτελεσμάτων από κάθε συνδυασμό απειλής, ευπάθειας, περιουσιακού στοιχείου και αντιμέτρου, καθορίζεται ο εναπομένων κίνδυνος. Εδώ, το στοιχείο της συνέπειας καλύπτεται στην αξία των περιουσιακών στοιχείων και το στοιχείο της πιθανότητας στις τιμές της απειλής και της ευπάθειας.

Παρόλα αυτά, είναι ευρέως αποδεκτό μεταξύ των επαγγελματιών της ασφάλειας πως δεν μπορεί να επιτευχθεί 100% ασφάλεια, ή με άλλα λόγια δεν είναι δυνατό να εκμηδενιστεί το ρίσκο. Ακόμη και αν υποθέσουμε πως είναι δυνατή η πλήρης εξάλειψη του ρίσκου, περιορισμοί του προϋπολογισμού παρεμποδίζουν το ενδεχόμενο αυτό, καθώς κάποια μέτρα κοστίζουν περισσότερο από την ίδια την αξία του περιουσιακού στοιχείου που πρέπει να προστατευθεί.

Λύση στο πρόβλημα αυτό δίνει η ανάλυση κινδύνων (risk analysis). Με τον όρο ανάλυση κινδύνων ενός πληροφοριακού συστήματος, νοείται, η διαδικασία αναγνώρισης και αξιολόγησης των κινδύνων ασφαλείας που εισάγει το σύστημα στην λειτουργία ενός οργανισμού, καθώς και το κόστος των απωλειών που θα προκληθούν σε περίπτωση που δημιουργηθεί πρόβλημα ασφαλείας. Έτσι προσδιορίζεται ο βαθμός κινδύνου του πληροφοριακού συστήματος και οι

απαιτήσεις ασφαλείας που υπάρχουν. Υπολογίζεται επιπλέον και το κόστος πρόληψης κάθε απώλειας ώστε να είναι δυνατή μια σωστή αντιμετώπιση των κινδύνων με ορθολογιστικά κριτήρια. Η ανάλυση κινδύνων έχει ως σκοπό την αξιολόγηση των περιουσιακών στοιχείων του οργανισμού και την αναγνώριση όλων των κινδύνων και των ευπαθειών που τα απειλούν.

Επιπρόσθετα, η ανάλυση κινδύνων θέτει προτεραιότητες στα αντίμετρα που μπορούν να εγκατασταθούν, με αποτέλεσμα να μπορεί να γίνει μια πιο ορθή επιλογή στις περιπτώσεις που ο προϋπολογισμός δεν επιτρέπει αρκετούς πόρους ώστε να καλυφθούν όλες οι ανάγκες για θέματα ασφαλείας. Ιδιαίτερα σήμερα που η παγκόσμια οικονομία βρίσκεται σε ύφεση και οι περισσότεροι οργανισμοί αναγκάζονται να κάνουν περικοπές σε όλους τους τομείς, η ανάλυση κινδύνων έρχεται να παίξει ουσιαστικό ρόλο στην σωστή αντιμετώπιση των προβλημάτων ασφαλείας με οργανωμένο και αποτελεσματικό τρόπο. Έτσι, η έμφαση για την αντιμετώπιση κινδύνων σε αυτό το πλαίσιο, μετατοπίζεται από την αποφυγή του κινδύνου στην διαχείριση κινδύνου. Η διαχείριση κινδύνου περιλαμβάνει τον προσδιορισμό, την επιλογή και την υιοθέτηση αντιμέτρων που δικαιολογούνται από τους εντοπιζόμενους κινδύνους των πόρων και την μείωση των εν λόγω κινδύνων σε αποδεκτά επίπεδα.

Ως εκ τούτου, στον τομέα της υγείας, ο σκοπός της ανάλυσης κινδύνου είναι να προσδιοριστεί πώς θα μπορούσε να επηρεαστεί ένα σύστημα από μία ενδεχόμενη παραβίαση της ασφάλειας και να καθοριστούν πόσο σοβαρές θα μπορούσαν να είναι οι συνέπειες για μία μονάδα υγείας. Αυτό παρέχει αιτιολόγηση για την ποσότητα και την φύση της προστασίας που απαιτείται.

Ένα ιδιαίτερο χαρακτηριστικό στον τομέα της υγείας επιδρά στο θέμα της ασφάλειας και επηρεάζει σημαντικά την πιθανότητα εμφάνισης πολλών απειλών. Αυτό είναι το γεγονός ότι είναι συχνά δύσκολο, αν όχι αδύνατο, να απομονωθούν οι πόροι του συστήματος από την ροή κυκλοφορίας των ασθενών και των επισκεπτών τους. Αυτό το χαρακτηριστικό από μόνο του αυξάνει το επίπεδο των απειλών.

4.3.1 Τεχνικές Ανάλυσης Κινδύνου

Υπάρχει ένας πολύ μεγάλος αριθμός από τεχνικές ανάλυσης κινδύνων. Αυτό οφείλεται στις διαφορετικές ανάγκες που χρειάζεται να καλύψουν. Γενικά όμως υπάρχουν δύο μεγάλες κατηγορίες για ανάλυση κινδύνων:

Ποσοτική ανάλυση: Η ποσοτική ανάλυση προσπαθεί να προσδιορίσει αντικειμενικές αριθμητικές τιμές (πχ. χρηματικά ποσά) για κάθε συνιστώσα της ανάλυσης κινδύνων. Για παράδειγμα προσπαθεί να υπολογίσει την χρηματική αξία των απωλειών ή την πιθανότητα (σε νούμερο) να συμβεί ένα περιστατικό. Στην περίπτωση που «ποσοτικοποιηθούν» όλες οι συνιστώσες (αξία περιουσιακών στοιχείων, συχνότητα απειλών, αποτελεσματικότητα αντίμετρων, κόστος

αντίμετρων, αβεβαιότητα και πιθανότητα) τότε η ανάλυση ονομάζεται πλήρως ποσοτική. Τα πλεονεκτήματα της τεχνικής αυτής είναι τα εξής:

- Τα αποτελέσματα έχουν το κύρος της μαθηματικής απόδειξης
- Τα αποτελέσματα μπορούν να εκφραστούν σε γλώσσα κατανοητή από τους διαχειριστές του οργανισμού
- Η ανάλυση κόστους/οφέλους (cost/benefit) είναι πιο εύκολη και άμεση.
- Η αξία των περιουσιακών στοιχείων του πληροφοριακού συστήματος (όσον αφορά την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) γίνεται καλύτερα κατανοητή όταν εκφράζεται σε χρηματικά ποσά. Αυτό βοηθάει στην μεγαλύτερη αποδοχή της ασφάλειας.

Παρόλα αυτά, μεταξύ αυτών διακρίνονται και κάποια μειονεκτήματα, τα οποία είναι:

- Οι υπολογισμοί μπορεί να είναι πολύπλοκοι
- Η ανάλυση χρειάζεται πολύ χρόνο για να ολοκληρωθεί
- Χρειάζεται μεγάλη ποσότητα προκαταρτικής εργασίας
- Η καθοδήγηση των συμμετεχόντων στην ανάλυση δεν μπορεί να γίνει εύκολα. Έτσι συνήθως χρειάζεται η συμμετοχή έμπειρων στην ποσοτική ανάλυση ατόμων.
- Ιστορικά, η ποσοτική ανάλυση λειτουργεί καλά μόνο με την χρήση κάποιου αυτοματοποιημένου εργαλείου συνδεδεμένου με μια γνωστική βάση (knowledge base).

Ιστορικά, η ποσοτική ανάλυση ήταν η πρώτη που χρησιμοποιήθηκε για την ανάλυση κινδύνων πληροφοριακών συστημάτων. Οι πρώτες προσπάθειες όμως συνάντησαν σημαντικές δυσκολίες λόγω της μεγάλης ποσότητας των δεδομένων και τις πολυπλοκότητας των υπολογισμών. Έτσι, ενώ πολλοί σχεδίασαν εργαλεία και αυτόματες διαδικασίες για την υποβοήθηση της ποσοτικής ανάλυσης, άλλοι κατέφυγαν στην δημιουργία πιο ποιοτικών μεθόδων ανάλυσης οι οποίες τελικά έγιναν και οι πιο διαδεδομένες.

Ποιοτική Ανάλυση: Η ποιοτική ανάλυση δεν προσπαθεί να δώσει ακριβείς αριθμητικές τιμές στις συνιστώσες της ανάλυσης κινδύνου. Αντιθέτως αρκείται να τις χαρακτηρίζει με εκφράσεις όπως πχ. μεγάλο, μέτριο, μικρό ή να δίνει τιμές από μια προαποφασισμένη κλίμακα. Με την λογική αυτή παρακάμπτονται οι πολύπλοκοι υπολογισμοί. Αν και οι κίνδυνοι δεν υπολογίζονται επακριβώς, επιτυγχάνεται η ταξινόμηση τους και επομένως η προτεραιότητα για την αντιμετώπιση τους. Η ποιοτική ανάλυση βασίζεται στην εμπειρία των ανθρώπων που συμμετέχουν για τον προσδιορισμό των κινδύνων. Πρόκειται προφανώς για μια υποκειμενική μέθοδος. Προσπαθεί να εκμεταλλευτεί την γνώση των ατόμων που συμμετέχουν ώστε να φτάσει σε αποδεκτά προσεγγιστικά αποτελέσματα στον ελάχιστο δυνατό χρόνο και με την ελάχιστη προσπάθεια, παρακάμπτοντας το πολύπλοκο μαθηματικό κομμάτι της ανάλυσης. Έχει αποδειχτεί με τον καιρό ότι η ποιοτική ανάλυση παράγει ικανοποιητικά αποτελέσματα όταν τα

άτομα που συμμετέχουν έχουν την απαιτούμενη γνώση και εμπειρία για το πληροφοριακό σύστημα που εξετάζεται. Όπως και η παραπάνω τεχνική, και αυτή χαρακτηρίζεται από μια σειρά πλεονεκτημάτων:

- Αποφεύγονται πολύπλοκοι υπολογισμοί
- Δεν είναι απαραίτητος ο αριθμητικός υπολογισμός της αξίας των περιουσιακών στοιχείων
- Είναι ευκολότερη η συμμετοχή ατόμων που δεν έχουν σχέση με την ασφάλεια και την πληροφορική.
- Η ποιοτική ανάλυση χρειάζεται λιγότερο χρόνο και λιγότερους πόρους σε σχέση με την ποσοτική
- Η διαδικασία της ανάλυσης είναι πιο ευέλικτη

Όμως, τα μειονεκτήματα που χαρακτηρίζουν την τεχνική αυτή είναι τα εξής:

- Είναι υποκειμενικής φύσεως
- Δεν γίνεται μεγάλη προσπάθεια για την αναγνώριση της αντικειμενικής αξίας των περιουσιακών στοιχείων. Έτσι, η αντίληψη της αξίας μπορεί να μην αντικατοπτρίζει την πραγματική αξία κατά τον υπολογισμό του κινδύνου.
- Η ποιότητα των αποτελεσμάτων βασίζεται εξολοκλήρου στην γνώση και την εμπειρία των ατόμων που συμμετέχουν στην ανάλυση
- Η ανάλυση κόστους/οφέλους (cost/benefit) δεν βασίζεται σε μαθηματική απόδειξη

Στην πραγματικότητα, οι περισσότερες τεχνικές που χρησιμοποιούνται σήμερα είναι μια μίξη ποσοτικής και ποιοτικής ανάλυσης. Τον χαρακτηρισμό ποιοτική ή ποσοτική ανάλυση την παίρνουν ανάλογα με ποια ανάλυση προσεγγίζουν καλύτερα.

4.3.2 Βασική Μεθοδολογία Ανάλυσης Κινδύνου

Ένας βασικός τύπος που αποτελεί την καρδιά της ανάλυσης κινδύνων είναι ο τύπος B>P*L. Τα τρία στοιχεία του τύπου BPL είναι:

- B = Το κόστος για την πρόληψη μιας απώλειας
- P = Η πιθανότητα να συμβεί μια απώλεια
- L = Το συνολικό κόστος μιας απώλειας

Το νόημα του τύπου είναι ότι, όταν το κόστος της πρόληψης μιας απώλειας είναι μεγαλύτερο από το γινόμενο του κόστους της απώλειας επί την πιθανότητα να συμβεί αυτή, τότε η υλοποίηση του μέτρου πρόληψης κρίνεται ως υπερβολική. Στην αντίθετη περίπτωση το μέτρο πρόληψης συμφέρει να υλοποιηθεί. Συνήθως τα μεγέθη υπολογίζονται σε ετήσιες απώλειες και ετήσια πιθανότητα να συμβεί ένα γεγονός. Ο τύπος αυτός αντικατοπτρίζει την κεντρική ιδέα

πίσω από κάθε ανάλυση κινδύνων, όχι μόνο για πληροφοριακά συστήματα. Συνεπώς, αποτελεί την ιδέα του υπολογισμού της πιο συμφέρουσας λύσης.

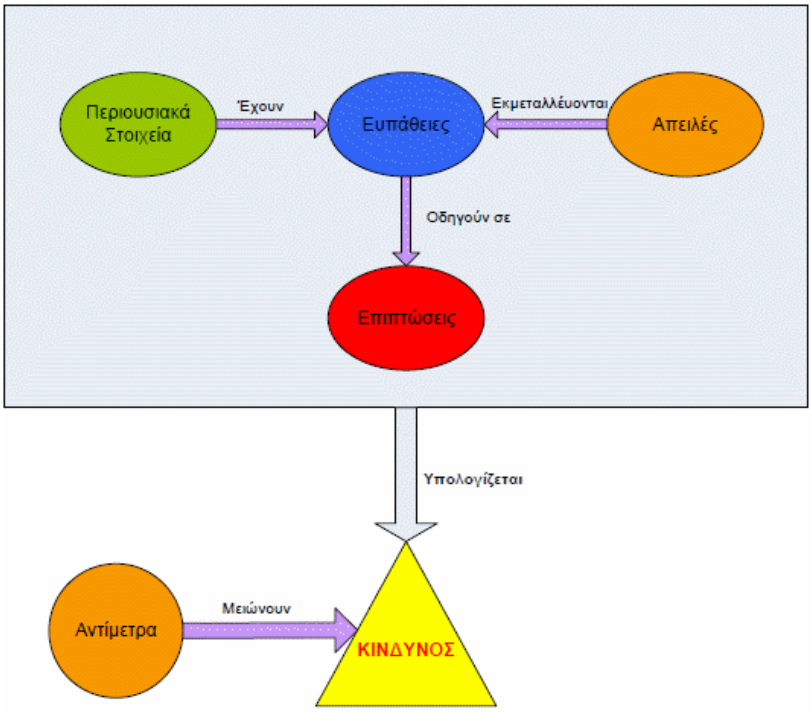
Ωστόσο, ο υπολογισμός του τύπου και η πρακτική του εφαρμογή βρίσκει σημαντικές δυσκολίες. Συγκεκριμένα, ο ακριβής υπολογισμός των τιμών των πιθανοτήτων και του κόστους πρόληψης ή απώλειας δεν είναι πάντα εύκολος ή δυνατός. Για παράδειγμα, η αντιστοίχηση των απωλειών με οικονομικά νούμερα δεν είναι πάντα δυνατή διότι πολλές φορές στην ανάλυση κινδύνων αξιολογούνται απώλειες απροσδιόριστες όπως η εικόνα ενός οργανισμού, η εμπιστοσύνη που έχουν οι «πελάτες» του σε αυτόν και στην περίπτωση των ΠΣΥ η απώλεια ζωής ενός ασθενή. Ακόμα και αν δεν χρησιμοποιείται όμως άμεσα, όλες οι μέθοδοι της ανάλυσης κινδύνων βασίζονται πάνω στην λογική του τύπου BPL.

Προκειμένου, λοιπόν, οι διαχειριστές να πάρουν σωστές αποφάσεις για την αποδοχή, αποτροπή ή μείωση των κινδύνων και την υλοποίηση αποδοτικών οικονομικά (cost effective) λύσεων ασφαλείας, είναι αναγκαία η υιοθέτηση μιας μεθοδολογίας που θα αντιμετωπίζει τα θέματα με βάση το κόστος και το όφελος. Με τον καιρό έχει δημιουργηθεί μια πληθώρα διαδικασιών που ήρθαν να καλύψουν διαφορετικές ανάγκες για ανάλυση κινδύνων. Αν και υπάρχουν πολλές διαφορετικές διαδικασίες, η βασική μέθοδος παραμένει η ίδια.

Ο κίνδυνος στον οποίο εκτίθεται ένα πληροφοριακό σύστημα είναι συνάρτηση:

- Της αξίας των περιουσιακών στοιχείων
- Των ευπαθειών του
- Των πιθανών απειλών και της φύσης τους
- Των επιπτώσεων που μπορεί να προκύψουν

Στο παρακάτω σχήμα φαίνονται οι σχέσεις μεταξύ των παραπάνω καθώς και η σχέση του κινδύνου με τα αντίμετρα που τελικά επιλέγονται.



Σχήμα 4.2 *Επικινδυνότητα και συναφείς όροι*

Η βασική μεθοδολογία της ανάλυσης κινδύνων περιλαμβάνει τα παρακάτω βήματα:

1. Καθορισμός του σκοπού και της εμβέλειας της ανάλυσης: Στο βήμα αυτό καθορίζεται τι ακριβώς θα περιληφθεί στην ανάλυση κινδύνων και ποια αποτελέσματα αναμένεται να παραχθούν από αυτήν.

2. Αναγνώριση και αξιολόγηση των περιουσιακών στοιχείων του πληροφοριακού συστήματος: Υπάρχουν πολλά περιουσιακά στοιχεία σε έναν οργανισμό, πολλά από τα οποία δεν είναι εύκολα αναγνωρίσιμα. Σε αυτό το βήμα γίνεται προσπάθεια αναγνώρισής τους και προσδιορισμός της αξίας τους προς τον οργανισμό.

3. Ανάλυση των απειλών προς τα περιουσιακά στοιχεία και των επιπτώσεων που μπορεί να έχουν: Για κάθε κατηγορία περιουσιακών στοιχείων υπάρχουν και μια σειρά από απειλές. Στο βήμα αυτό αναγνωρίζονται οι απειλές για κάθε περιουσιακό στοιχείο, ο τρόπος με τον οποίο το απειλούν και οι επιπτώσεις που θα επιφέρει η κάθε απειλή.

4. Ανάλυση των ευπαθειών: Ένα περιουσιακό στοιχείο μπορεί να είναι λιγότερο ευπαθής προς μια απειλή και περισσότερο προς μια άλλη. Στο βήμα αυτό διευκρινίζεται η ευπάθεια του κάθε περιουσιακού στοιχείου προς κάθε απειλή ξεχωριστά. Η ευπάθεια μπορεί να οριστεί και με την εξής συνάρτηση:

Ευπάθεια = Πιθανότητα να συμβεί μια απειλή x Πιθανότητα να είναι επιτυχής

5. Υπολογισμός του κινδύνου: Ο βαθμός του κινδύνου υπολογίζεται ξεχωριστά για κάθε απειλή προς κάθε περιουσιακό στοιχείο. Είναι συνάρτηση όλων των παραπάνω, δηλαδή:

- Των επιπτώσεων μιας απειλής (που έχουν σχέση με την αξία του περιουσιακού στοιχείου)
- Της ευπάθειας του περιουσιακού στοιχείου ως προς την απειλή.

6. Επιλογή τρόπων αντιμετώπισης των κινδύνων: Υπάρχουν 3 τρόποι αντιμετώπισης του κινδύνου:

- Αποφυγή του κινδύνου με πλήρη απόσυρση από μια συγκεκριμένη δραστηριότητα
- Αποδοχή του κινδύνου
- Μείωση του κινδύνου με χρήση αντιμέτρων (μέτρων ασφαλείας)

Με τα αντίμετρα μπορούν να επιτευχθούν τα εξής:

- Μεταφορά κινδύνου, πχ αγορά ασφάλειας
- Μείωση ευπάθειας:
  - Μείωση πιθανότητας να συμβεί μια απειλή πχ απαγορεύοντας το κάπνισμα σε μια ευαίσθητη περιοχή.
  - Μείωση πιθανότητας μια απειλή να είναι επιτυχής πχ χρήση κρυπτογράφησης, χρήση αναχώματος.
- Μείωση αντίκτυπου, πχ σύστημα πυρόσβεσης
- Μέτρα ανάνηψης (επαναφοράς), πχ backup

Κατά το βήμα αυτό αναγνωρίζονται τα πιθανά αντίμετρα που μπορούν να εφαρμοστούν και επιλέγονται αυτά που συμφέρουν περισσότερο στον οργανισμό.

7. Τα επόμενα βήματα: Η ανάλυση κινδύνων και η ασφάλεια των πληροφοριακών συστημάτων γενικότερα είναι μια συνεχόμενη διαδικασία. Μετά την επιλογή των τρόπων αντιμετώπισης και την εφαρμογή τους στον οργανισμό πρέπει να υπάρχει μια συνεχής παρακολούθηση των κινδύνων. Τα δεδομένα σε ένα πληροφοριακό σύστημα αλλάζουν συνεχώς, εισάγονται νέες απειλές, νέες ευπάθειες, νέες επιπτώσεις κτλ. Τα αντίμετρα που έχουν επιλεχθεί ελέγχονται συνεχώς για την αποτελεσματικότητα τους. Πολλά από αυτά με τον καιρό σταματούν να συμφέρουν στον οργανισμό και πρέπει να καταργηθούν ή να αντικατασταθούν από νέα αντίμετρα.

4.3.3 Μεθοδολογίες Ανάλυσης Κινδύνου

Η ανάλυση κινδύνων δεν είναι απλή διαδικασία και συνήθως παράγει ένα πολύ μεγάλο αριθμό δεδομένων για επεξεργασία. Όσο μεγαλύτερο δε το εύρος της ανάλυσης, τόσο πιο δύσκολη είναι η διαχείριση των πληροφοριών που συλλέγονται. Αναγνωρίζοντας την παραπάνω δυσκολία,

πολλές εταιρίες έχουν αναπτύξει μεθοδολογίες για την διευκόλυνση της ανάλυσης κινδύνων. Οι καταξιωμένες μεθοδολογίες ανάλυσης κινδύνων διέπονται από μια σειρά πλεονεκτημάτων και μειονεκτημάτων, αρχές αλλά και περιορισμούς, όταν εφαρμόζονται σε σύγχρονα πληροφοριακά συστήματα. Παρακάτω περιγράφονται τα βασικά χαρακτηριστικά και δυνατότητες που προσφέρουν τα σύγχρονα πακέτα λογισμικού ανάλυσης κινδύνων και γίνεται μια προσπάθεια παρουσίασης μερικών από αυτών.

Η μεθοδολογία CRAMM είναι ένα εργαλείο ποιοτικής ανάλυσης κινδύνων που αναπτύχθηκε από το CCTA (Central Computer and Telecommunications Agency) της βρετανικής κυβέρνησης το 1985 ώστε να εφοδιάσει τα διάφορα τμήματα της κυβέρνησης με μια κοινή μέθοδο ανάλυσης κινδύνων πληροφοριακών συστημάτων. Το πρόγραμμα έχει υποστεί σημαντικές αναθεωρήσεις και συνεχίζει να αναπτύσσεται πλέον από την εμπορική εταιρία Insight Consulting που έχει έδρα στην Αγγλία. Η CRAMM έχει μεγάλο κύρος, καθώς χρησιμοποιείται σε παραπάνω από 500 οργανισμούς σε 23 χώρες, συμπεριλαμβανομένου και του ΝΑΤΟ. Το πρόγραμμα ακολουθεί την δική του μέθοδο, η οποία αποτιμά και βοηθάει τους οργανισμούς να επιτύχουν συμμόρφωση με το διεθνές πρότυπο ISO17799/BS7799.

Η μεθοδολογία CRAMM μπορεί να χρησιμοποιηθεί για την αναγνώριση, ανάλυση και διαχείριση κινδύνων όσον αφορά πληροφοριακά συστήματα, όπως αυτά της υγείας. Συγκεκριμένα, περιλαμβάνει την πιθανότητα ύπαρξης ανεπιθύμητου συμβάντος, όπως για παράδειγμα αυτό της αποθήκευσης λανθασμένων δεδομένων ενός ασθενή, καθώς και τις συνέπειες ενός τέτοιου περιστατικού, όπως για παράδειγμα η λανθασμένη θεραπεία του ασθενούς αυτού. Η μεθοδολογία αυτή τονίζει τα ζητήματα ασφάλειας και προετοιμάζει το έδαφος ώστε να συμπεριληφθούν κατάλληλες τεχνικές ως αντίμετρα, εφόσον και όταν κριθούν απαραίτητα. Συνεπώς, η CRAMM περιλαμβάνει τρείς φάσεις:

- Αναγνώριση και εκτίμηση πόρων- περιουσιακών στοιχείων
- Αναγνώριση και εκτίμηση απειλών και ευπαθειών
- Επιλογή αντιμέτρων

Επιπλέον, τα βασικά χαρακτηριστικά της μεθοδολογίας αυτής είναι:

- Τεράστια βάση αντιμέτρων (3000 αντίμετρα) που καλύπτει όλες τις πτυχές της ασφάλειας πληροφοριακών συστημάτων. Η βάση ανανεώνεται συνεχώς.
- «What if» ανάλυση
- Εργαλεία για την δημιουργία σχεδίων Επιχειρησιακής Συνέχειας (Business Continuity)
- Οδηγοί για την δημιουργία πολιτικών ασφαλείας
- Οδηγοί για την δημιουργία αναφορών με δυνατότητες χάραξης πινάκων και γραφημάτων και εξαγωγής τους σε διάφορες μορφές αρχείων
- Σχετικά σύγχρονο περιβάλλον σε πλατφόρμα MS Windows

- Δυνατότητα προσαρμογής του προγράμματος στις ανάγκες του κάθε οργανισμού

Ένα από τα μειονεκτήματα της CRAMM είναι η όχι και τόσο απλή χρήση της, με αποτέλεσμα να απαιτείται εκπαίδευση και εξοικείωση για να επιτευχθούν τα βέλτιστα αποτελέσματα. Τέλος, υπάρχει και η έκδοση CRAMM Express η οποία δεν περιλαμβάνει όλα τα εργαλεία σαν την κανονική έκδοση αλλά είναι πιο απλή στην χρήση και οδηγεί σε πιο γρήγορα αλλά λιγότερο αναλυτικά αποτελέσματα.

Η ODESSA, μια πιο πρόσφατη μεθοδολογία ανάλυσης κινδύνων, αναπτύχθηκε ειδικά για την χρήση της στον τομέα της υγείας. Η ιδέα του συστήματος της ODESSA είναι ότι, σε βασικό επίπεδο, όλοι οι οργανισμοί να έχουν παρόμοιες απαιτήσεις ασφάλειας, αλλά πέρα από αυτό το βασικό επίπεδο, τα αντίμετρα ασφάλειας να είναι μοναδικά για κάθε οργανισμό. Τα βασικά αντίμετρα αναφέρονται στις ελάχιστα αποδεκτές απαιτήσεις ασφάλειας για οποιοδήποτε είδος οργανισμού (νοσοκομείο, παθολόγος, φαρμακείο και τα συναφή). Αυτά τα αντίμετρα εξαρτώνται από το περιβάλλον του κάθε οργανισμού (πχ από την τοποθεσία των πόρων του οργανισμού υγείας, όπως το κέντρο της πόλης), και από το είδος του οργανισμού (πχ ένα νοσοκομείο). Ένα σύνολο από μοναδικές απαιτήσεις ασφάλειας για έναν συγκεκριμένο οργανισμό υγείας, μπορεί να συνταθεί με τον συνδυασμό αυτών των βασικών αντιμέτρων και των συγκεκριμένων απαιτήσεων του κάθε οργανισμού υγείας.

Η μεθοδολογία ODESSA απλοποιεί την αναγνώριση των απαιτήσεων ασφάλειας για κάθε ΠΣΥ ξεχωριστά και παρέχει την δυνατότητα στον διαχειριστή του συστήματος να επιλέξει τα κατάλληλα αντίμετρα ασφάλειας για το σύστημά του.

Η μεθοδολογία OCTAVE αναπτύχθηκε από το Software Engineering Institute (SEI) του πανεπιστημίου Carnegie Mellon. Η μεθοδολογία OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) παρέχει μια ολοκληρωμένη διαδικασία που συμπεριλαμβάνει οδηγίες, λίστες ελέγχου, χρονικές εκτιμήσεις και περιγραφές διαδικασιών των τριών φάσεων που την χαρακτηρίζουν. Οι τρεις αυτές φάσεις περιλαμβάνουν (Landoll, 2006):

- Δημιουργία προφίλ απειλών βάσει των πόρων
- Αναγνώριση των ευπαθειών της υποδομής
- Ανάπτυξη σχεδίου ασφάλειας και στρατηγικής

Η OCTAVE μπορεί να χρησιμοποιηθεί σε σχετικά μικρούς και απροετοίμαστους οργανισμούς. Επιπλέον, έχει προταθεί από το HIPAA των ΗΠΑ ως η πλέον καταλληλότερη μεθοδολογία για την εκτίμηση κινδύνων σε συμβόλαια ασφάλειας υγείας.

Άλλες ευρέως χρησιμοποιούμενες μεθοδολογίες είναι:

- FRAP: Facilitated Risk Assessment Process
- COBIT: Control Objectives for Information and related Technology

- DRAM (Delphi Risk Assessment Method)

Για την παροχή υψηλής κλιμάκωσης και επαναληψιμότητας της διαδικασίας ανάλυσης κινδύνου, κάθε μεθοδολογία απαιτεί την εκτεταμένη και προτυποποιημένη τεκμηρίωση καθ' όλη την διάρκεια της ανάλυσης. Επιπλέον, κάθε ανάλυση κινδύνου είναι μια πολύπλοκη διαδικασία που απαιτεί μια γνωστική ομάδα με ευρύ πεδίο δεξιοτήτων και εμπειρίας. Η προσπάθεια εφαρμογής των μεθόδων αυτών, απαιτεί μια σημαντική επένδυση σε ανθρώπινο δυναμικό και σε αφιέρωση χρόνου για την εφαρμογή, την εκπαίδευση χρηστών και την διαχείριση τεκμηρίων. Παρόλο που οι μεθοδολογίες αυτές είναι ωφέλιμες και εφαρμόσιμες σε μερικούς οργανισμούς, μια ώριμη διαδικασία ανάλυσης κινδύνου πρέπει να είναι ευρέως αποδεκτή στα πλαίσια του οργανισμού, πριν την απόπειρα εφαρμογής τέτοιων αυστηρών μεθόδων, χωρίς να αγνοείται το γεγονός ότι καθεμία είναι άμεσα συνδεδεμένη με την επιβάρυνση της εκπαίδευσης, τεκμηρίωσης και εφαρμογής (πχ άνθρωποι, χρόνος και χρήματα).

4.3.4 Κρίσιμα Ζητήματα των Μεθόδων Ανάλυσης Κινδύνων σε ΠΣΥ

Ο σκοπός ενός οργανισμού υγείας είναι η φροντίδα του ασθενή. Συνεπώς, το πιο σημαντικό «περιουσιακό στοιχείο» του οργανισμού υγείας είναι ο ασθενής, σε αντίθεση, για παράδειγμα, με έναν οργανισμό οικονομικών, όπου το πιο σημαντικό περιουσιακό στοιχείο είναι οι οικονομικοί πόροι. Εξίσου σημαντική είναι η ανάγκη για την προστασία της ιδιωτικότητας του ασθενή κατά την ανταλλαγή των δεδομένων του ασθενή, προκειμένου να διασφαλιστεί η διαθεσιμότητα ακριβών και εγκαίρων πληροφοριών σε όλους τους εξουσιοδοτημένους επικοινωνούντων εταίρων.

Το κατανεμημένο περιβάλλον υγείας αυξάνει την πιθανότητα εμφάνισης κινδύνων, εξαιτίας του γεγονότος ότι πολλοί από τους εταίρους που επικοινωνούν μπορεί να είναι αναξιόπιστοι. Οι περισσότερες από τις συνέπειες από την ύπαρξη απειλών σε ΠΣΥ, είναι δύσκολο να ποσοτικοποιηθούν, εξαιτίας της μη οικονομικής φύσεώς τους. Για παράδειγμα, είναι δύσκολο να καθοριστεί το κόστος που συνδέεται με την λανθασμένη θεραπεία ενός ασθενή, αν τα δεδομένα που αποθηκεύονται δεν είναι ακριβή. Συνεπώς, είναι επιτακτική η ανάγκη να βρεθεί τρόπος που να καθορίζει επακριβώς αυτό το μη οικονομικό κόστος. Η ανάγκη αυτή εισάγει ένα είδος ασάφειας όσον αφορά την εισαγωγή δεδομένων που απαιτείται από ένα ΠΣΥ.

Άλλο ένα κρίσιμο ζήτημα που αφορά τις ευπάθειες που εισάγονται σε έναν οργανισμό υγείας, είναι η υποβολή του σε μοναδικές εκθέσεις, όπως ιατρική αναξιοπιστία επαγγελματιών, λάθη διαχείρισης φροντίδας και η αντιμετώπιση επειγόντων καταστάσεων οι οποίες διαφέρουν σημαντικά από άλλους οργανισμούς. Για παράδειγμα, όταν ένας ασθενής εισάγεται στην μονάδα επειγόντων περιστατικών ενός νοσοκομείου, είναι αναγκαίο τα δεδομένα του να είναι άμεσα

διαθέσιμα για τη σωστή του θεραπεία. Η έλλειψη της διαθεσιμότητας και της ακεραιότητας των δεδομένων του ασθενή θα μπορούσε να οδηγήσει σε απώλεια ζωής.

Ως εκ τούτου, κάποια από τα ζητήματα που πρέπει να θεωρηθούν όσον αφορά τη χρήση των τωρινών μοντέλων ανάλυσης κινδύνων σε ΠΣΥ είναι τα εξής:

- Αν οι απειλές, οι οποίες προβλέπονται σε τωρινές μεθοδολογίες ανάλυσης κινδύνων, είναι αντιπροσωπευτικές για τις απειλές που εμφανίζονται σε περιβάλλοντα υγείας.
- Αν τα αντίμετρα που προτείνονται από τα τωρινά μοντέλα ανάλυσης κινδύνων, είναι εφαρμόσιμα και σε ΠΣΥ.
- Αν οι μέθοδοι που χρησιμοποιούνται για την εκτέλεση ανάλυσης κινδύνων είναι επιστημονικές και κατάλληλες για ΠΣΥ.

Παρόλο που αναλύσεις κινδύνων έχουν εφαρμοστεί επιτυχώς στον τομέα της υγείας, άλλοι τομείς μπορούν να συνεισφέρουν στην βελτίωση των τωρινών μεθόδων ανάλυσης κινδύνων σε ΠΣΥ. Όλα τα προαναφερθέντα χαρακτηριστικά οφείλεται να ενσωματωθούν στην διαδικασία ανάλυσης κινδύνων ενός ΠΣΥ. Έτσι, τα υπάρχοντα μοντέλα ανάλυσης κινδύνων μπορούν να προσαρμοστούν με σκοπό την περεταίρω βελτίωση της διαδικασίας ανάλυσης κινδύνων σε περιβάλλοντα υγείας.

4.4 Πολιτικές Ασφάλειας σε Οργανισμούς Υγείας

Η πολιτική ασφάλειας ορίζεται ως η περιγραφή του συνόλου των κανόνων, των προτύπων και των διαδικασιών που καθορίζουν τα φυσικά, διαδικαστικά, τεχνικά και προσωπικά μέτρα ασφάλειας που λαμβάνονται στη διοίκηση, τη διανομή και την προστασία των περιουσιακών στοιχείων. Με την ολοκλήρωση της ανάλυσης κινδύνων, αναπτύσσεται μια πολιτική ασφάλειας, η οποία και θα καθορίσει το πώς θα αντιμετωπιστούν οι κίνδυνοι που αναγνωρίστηκαν και αποτιμήθηκαν.

Οι πολιτικές ασφάλειας περιλαμβάνουν μια σειρά από γενικευμένες απαιτήσεις που έχουν εγκριθεί στο διοικητικό επίπεδο του οργανισμού υγείας, και που υποδεικνύουν ένα σχέδιο δράσης για το προσωπικό που οφείλει να λαμβάνει αποφάσεις. Επιπλέον, καθώς οι κίνδυνοι αλλάζουν και πρέπει να επανεκτιμούνται, έτσι και οι πολιτικές ασφάλειας θα πρέπει να αναθεωρούνται σε ετήσια βάση. Πρότυπα, διαδικασίες και κατευθυντήριες γραμμές συμπληρώνουν τις εν λόγω απαιτήσεις, με την προσαρμογή των πολιτικών σε συγκεκριμένα τμήματα. Τα πρότυπα δηλώνουν τις ελάχιστες προδιαγραφές που υπαγορεύονται από τις πολιτικές μιας οντότητας. Οι διαδικασίες δίνουν μια μέθοδο και οδηγίες με τις οποίες μια πολιτική ολοκληρώνεται. Οι διαδικασίες, κατά κανόνα, προσαρμόζονται σε κάθε κατάλληλο τμήμα, καθώς δεν οφείλουν όλα τα τμήματα να πληρούν τις απαιτήσεις μιας πολιτικής στο ίδιο ορισμένο

επίπεδο. Τέλος, οι κατευθυντήριες γραμμές είναι προτάσεις για την εκπλήρωση συγκεκριμένων καθηκόντων. Συγκεκριμένα, το HIPAA απαιτεί τεκμηρίωση για τις πολιτικές, τα πρότυπα και τις διαδικασίες ως επαλήθευση ότι οι οργανισμοί υγείας βρίσκονται σε συμμόρφωση με τον κανονισμό.

Ένα καλό υπόδειγμα για το περιεχόμενο μιας πολιτικής είναι:

1. Στόχος της πολιτικής: μια σύντομη δήλωση σχετική με το τι επιδιώκουμε να επιτευχθεί με την εφαρμογή της πολιτικής.
2. Σκοπός της πολιτικής: περιλαμβάνει σε γενικές γραμμές τον λόγο για τον οποίο υιοθετήθηκε και τον τρόπο με τον οποίο θα εφαρμοστεί.
3. Κοινό: σε ποιους τομείς εφαρμόζεται η πολιτική.
4. Δήλωση Πολιτικής: ορίζεται η δομή της πολιτικής (λεπτομέρειες για τον τρόπο με τον οποίο θα υλοποιηθεί).
5. Εξαιρέσεις από την πολιτική.
6. Ορισμοί (εφόσον και αν απαιτούνται).
7. Στοιχεία επικοινωνίας για ερωτήσεις και επεξηγήσεις.

Κάθε οργανισμός που δημιουργεί, χρησιμοποιεί, αποθηκεύει και κοινοποιεί πληροφορίες υγειονομικής περίθαλψης έχει νομική και ηθική ευθύνη να τιμήσει τη εμπιστοσύνη των ασθενών. Από την άλλη μεριά, η δημόσια πολιτική, οι νόμοι, οι ρυθμιστικές απαιτήσεις, οι απαιτήσεις διαπίστευσης και οι προσδοκίες των ασθενών απαιτούν ορισμένα πρότυπα για την ασφάλεια πληροφοριών. Ωστόσο, η μοναδική αποστολή, κουλτούρα και διαχείριση του κάθε οργανισμού επηρεάζει σημαντικά τις πολιτικές που ένας συγκεκριμένος οργανισμός αναπτύσσει για την προστασία της εμπιστευτικότητας, ακεραιότητας, και διαθεσιμότητας των πληροφοριών ασθενών και των πληροφοριών διοίκησης.

Οι ολοκληρωμένες πολιτικές ασφάλειας πληροφοριών αποτελούν τη βάση για ένα επιτυχημένο πρόγραμμα ασφάλειας πληροφοριών. Αυτές οι πολιτικές πρέπει να καθορίζουν τη φιλοσοφία και την κατεύθυνση του οργανισμού ως προς την προστασία των πληροφοριών καθώς και να τεκμηριώνονται και να κοινοποιούνται σε ολόκληρο τον οργανισμό.

4.5 Απειλές ενάντια της Ασφάλειας και Ιδιωτικότητας σε ΠΣΥ

Τα τελευταία χρόνια, ο αριθμός των απειλών στον τομέα των ΠΣΥ έχει αυξηθεί δραματικά καθώς η έλλειψη επαρκών μέτρων ασφάλειας έχει προκαλέσει πολυάριθμες παραβιάσεις δεδομένων, αφήνοντας τους ασθενείς εκτεθειμένους σε οικονομικές απειλές, ψυχική οδύνη ίσως και κοινωνικό στίγμα. Με την κατανόηση των απειλών ενάντια της ασφάλειας των πληροφοριών υγείας, ένας οργανισμός μπορεί να ενισχύσει το επίπεδο προστασίας των πληροφοριών σε ένα ΠΣΥ. Συνεπώς, ζητήματα που αφορούν την ασφάλεια, την αναγνώριση και ταξινόμηση απειλών

στον τομέα των οργανισμών υγειονομικής περίθαλψης, αποτελούν σημαντικές και υποχρεωτικές παράμετροι για τα ΠΣΥ. Παρακάτω παρουσιάζεται μια ολοκληρωμένη ανασκόπηση της βιβλιογραφίας των απειλών σε ΠΣΥ.

Η ετήσια έρευνα για το έγκλημα πληροφορικής και ασφάλειας του CSI/FBI κατάταξε ως σημαντικές απειλές τις εξής: Ιοί, Κατάχρηση μελών της πρόσβασής τους στο δίκτυο, Lap-top, Άρνηση υπηρεσιών (DoS), Μη εξουσιοδοτημένη πρόσβαση από μέλη, Διείσδυση συστημάτων, Κλοπή ιδιόκτητων πληροφοριών, Οικονομική απάτη, Απάτη τηλεπικοινωνιών, Δολιοφθορά, Κρυφάκουσμα τηλεπικοινωνιών, και Ενεργές υποκλοπές.

Σύμφωνα με τον T.C Rindfleisch, οι σημαντικότερες απειλές ενάντια στην εμπιστευτικότητα των ασθενών είναι: Αθέμιτη αποκάλυψη, Περιέργεια των μελών, Δωροδοκία μελών με σκοπό το κέρδος, Ανεξέλεγκτη δευτερογενή χρήση, και Μη εξουσιοδοτημένη πρόσβαση. Ο NIST 800-30 παρέχει μια κατηγοριοποίηση των πηγών απειλής που διακρίνονται σε έξι σημεία: Ανθρώπινη πρόθεση, Χωρίς πρόθεση ανθρώπινη ενέργεια, Τεχνική απειλή, Λειτουργική απειλή, Περιβαλλοντική απειλή, και Φυσική απειλή.

Πρόσφατες έρευνες δείχνουν ότι οι απειλές ενάντια της ιδιωτικότητας των ασθενών και της ασφάλειας των πληροφοριών μπορούν να ταξινομηθούν σε δυο ευρύτερους τομείς:

- Οργανωτικές απειλές
- Συστηματικές απειλές

Πρόσφατες μελέτες δείχνουν ότι το ευρύ φάσμα οργανωτικών απειλών θα μπορούσε να ταξινομηθεί σε πέντε επίπεδα, κατά αύξουσα σειρά πολυπλοκότητας (NRC 1997; Ribdfleisch 1997):

- Αθέμιτη αποκάλυψη: το προσωπικό υγειονομικής περίθαλψης αποκαλύπτει ακούσια τις πληροφορίες ασθενών σε άλλους πχ μήνυμα ηλεκτρονικού ταχυδρομείου που αποστέλλεται σε λάθος διεύθυνση ή διαρροή πληροφοριών μέσω της ανταλλαγής αρχείων peer-to peer.
- Περιέργεια μελών του οργανισμού: ένα μέλος με προνόμια πρόσβασης εξετάζει τα αρχεία ασθενών από περιέργεια ή για δικό του σκοπό πχ η πρόσβαση μιας νοσοκόμας στις πληροφορίες συναδέλφου της για να προσδιορίσει την πιθανότητα σεξουαλικά μεταδιδόμενης ασθένειας στον συνάδελφο ή η πρόσβαση ιατρικού προσωπικού σε ενδεχομένως ενοχλητικές πληροφορίες υγείας μιας διασημότητας και η διαβίβασή τους στα μέσα μαζικής ενημέρωσης.
- Παραβίαση δεδομένων από κάποιο μέλος του οργανισμού: μέλη του οργανισμού που έχουν πρόσβαση στις πληροφορίες ασθενών και τις διαβιβάζουν σε τρίτους με σκοπό το κέρδος ή την εκδίκηση του ασθενούς.

- Παραβίαση δεδομένων από τρίτους με φυσική εισβολή: ένας τρίτος που εισέρχεται στη φυσική εγκατάσταση με εξαναγκασμό ή αναγκαστική είσοδο και αποκτά πρόσβαση στο σύστημα.
- Μη εξουσιοδοτημένη εισβολή του συστήματος δικτύου: ένας τρίτος, συμπεριλαμβανομένων των πρώην εκδικητικών υπαλλήλων, ασθενών ή χάκερ, που εισβάλλει στο σύστημα δικτύου του οργανισμού από το εξωτερικό του, για να αποκτήσει πρόσβαση σε πληροφορίες ασθενών ή να καταστήσει το σύστημα εκτός λειτουργίας.

Πίνακας 4.1 *Πιθανοί συνδυασμοί δικαιωμάτων πρόσβασης στην παραβίαση δεδομένων υγείας*

Level of Access	**Example**
None	Outside Attacker
Site only	Maintenance worker
Site and System	Employee in the billing department who has access to information systems but not to clinical information
Data and System	Vendor or consultant with remote access privileges
Site, System, and Data	Care provider such as doctor or nurse

Όσον αφορά τις συστηματικές απειλές, ο Etzioni (1999) θέτει ως ισχυρό επιχείρημα ότι μια σημαντική απειλή ενάντια στην ιδιωτικότητα του ασθενή δεν εμφανίζεται εκτός της αλυσίδας ροής πληροφοριών στον τομέα της υγείας, αλλά από μέλη που νόμιμα έχουν πρόσβαση στις πληροφορίες ασθενών. Για παράδειγμα, οι ασφαλιστικές εταιρείες μπορούν να αρνηθούν την ασφάλιση ζωής σε ασθενείς με βάση την ιατρική τους κατάσταση, ή ένας εργοδότης, έχοντας πρόσβαση στο ιατρικό ιστορικό των εργαζομένων του, μπορεί να αρνηθεί την προαγωγή, ή ακόμη χειρότερα, να τερματίσει την απασχόληση. Οι ασθενείς ή/και οι οργανισμοί πληρωμής μπορούν να υποστούν οικονομικές απώλειες ως αποτέλεσμα των αθέμιτων πρακτικών και της παροχής περιττών ιατρικών υπηρεσιών.

Μια ταξινόμηση των απειλών Πληροφοριακών Συστημάτων (ΠΣ), όπως αυτά της υγείας, παρουσιάζεται από τον Whitman και αποτελείται από δώδεκα σημεία. Στο πλαίσιο αυτό, επισήμανε την προτεραιότητα των δαπανών και για την προστασία των ΠΣ από αυτές τις απειλές παρείχε μια online έρευνα, όπου ζητούσε από στελέχη πληροφορικής να ταξινομήσουν τις απειλές της ασφάλειας πληροφοριών. Τα ευρήματα έδειξαν ότι η πιο κρίσιμη απειλή για τα ΠΣ είναι οι «σκόπιμες επιθέσεις λογισμικού» που θεωρείται σχεδόν δύο φορές πιο σημαντική σε σύγκριση με την δεύτερη απειλή στη λίστα. Τεχνικές βλάβες ή σφάλματα λογισμικού, πράξεις ανθρώπινου λάθους, σκόπιμες πράξεις κατασκοπείας ή παραβίασης, επισημάνθηκαν επίσης ως υψηλού κινδύνου απειλές για τα ΠΣΥ.

Κάθε οργανισμός θα πρέπει να δώσει προτεραιότητα στις απειλές που αντιμετωπίζει με βάση την συγκεκριμένη κατάσταση ασφάλειας μέσα στην οποία δραστηριοποιείται, την οργανωτική στρατηγική του όσον αφορά τον κίνδυνο και τα επίπεδα έκθεσης μέσα στα οποία τα περιουσιακά του στοιχεία λειτουργούν. Επομένως, άλλο ένα σύστημα κατηγοριοποίησης έχει γίνει που αποτελείται από δεκατέσσερις γενικές κατηγορίες και αντιπροσωπεύει τους σαφείς και παρόντες κινδύνους που διατρέχουν οι άνθρωποι, οι πληροφορίες και τα συστήματα ενός οργανισμού. Τα αποτελέσματα είναι γενικά παρόμοια με προηγούμενες μελέτες στις οποίες οι επιθέσεις κατασκοπείας ή παραβίασης και οι επιθέσεις λογισμικού παραμένουν στην κορυφή της λίστας και το ανθρώπινο λάθος ή η ανθρώπινη παράλειψη καταλαμβάνουν την τρίτη θέση. Μετά από αυτές, υπάρχουν νέες επιλογές που προστίθενται στην τελευταία κατηγορία και συγκεκριμένα: Ελλείπουσα ανεπαρκής ή ελλιπής οργανωτική πολιτική ή Προγραμματισμός και ελλείποντες ανεπαρκείς ή ελλιπείς έλεγχοι. Οι Yeh και Chang προσδιορίζουν επίσης πενήντα θεμελιώδη αντίμετρα ασφάλειας που υιοθετούνται συνήθως για να αξιολογήσουν την επάρκεια ασφάλειας ΠΣ σε επτά κατηγορίες.

Σύμφωνα με τους Whitman και Mattord, στη λίστα που ακολουθεί, οι σημαντικές απειλές έχουν ταξινομηθεί από την Έρευνα για το Ετήσιο Έγκλημα Πληροφορικής και Ασφάλειας (Annual Computer Crime and Security Survey) το 2008: Άρνηση υπηρεσιών (DoS), Κλοπή φορητών υπολογιστών, Απάτη τηλεπικοινωνιών, Μη εξουσιοδοτημένη πρόσβαση, Ιός, Οικονομική απάτη, Κατάχρηση μελών, Διείσδυση συστημάτων, Δολιοφθορά, Κλοπή/Απώλεια ιδιόκτητων πληροφοριών, Κατάχρηση του ασύρματου δικτύου, Παραμόρφωση ιστοχώρου, Κακή χρήση των εφαρμογών ιστού, Bots, DNS επιθέσεις, Κατάχρηση στιγμιαίου μηνύματος, Password Sniffing, Απώλεια/Κλοπή των δεδομένων των πελατών. Επιπλέον, το πρότυπο ISO/IEC 27002, επίσης, εξετάζει ένδεκα τυποποιημένους τομείς που σχετίζονται με την διαχείριση της ασφάλειας πληροφοριών.

Με μελέτη που διεξήχθη από τους Narayana Samy et al., ανακαλύφθηκε ότι υπάρχουν συνολικά 22 τύποι απειλών σε ένα Ολοκληρωμένο Πληροφοριακό Σύστημα Νοσοκομείου (ΟΠΣΝ) (Total Hospital Information System-THIS), και απαρίθμησε τις κρίσιμες απειλές σε ένα ΠΣΥ. Ένα χρόνο αργότερα, σε μια άλλη μελέτη, εξέτασαν την κατηγοριοποίηση που απαριθμήθηκε σε ένα νοσοκομείο στη Μαλαισία. Τα αποτελέσματα παρουσίασαν τις κρισιμότερες απειλές μαζί με την ταξινόμησή τους.

Οι Pardue και Partidar από την άλλη, αναπαριστούν μια πρώτη προσπάθεια καταγραφής απειλών ενάντια των ηλεκτρονικών δεδομένων υγειονομικής περίθαλψης που συνδέονται με την μη εξουσιοδοτημένη πρόσβαση, την απώλεια και την διαφθορά δεδομένων, η οποία προκαλείται από βανδαλισμούς, απώλεια ή καταστροφή δεδομένων, λόγω ελαττωματικού υλικού ή λογισμικού, ανθρώπινου λάθους, κακόβουλου λογισμικού, φυσικής καταστροφής και της επίθεσης βάσεων δεδομένων.

Άλλο ένα πρότυπο δένδρο απειλών (threat tree) οργανώθηκε γύρω από τον στόχο ενός επιτιθέμενου, ή της έκβασης μιας απειλής, ανάλογα με το αν η απειλή είναι σκόπιμη ή όχι. (J.P Laundry et al., 2011).

Κατόπιν, ο Kortz παρείχε μια ταξινόμηση που αποτελείται από 25 απειλές, οργανωμένη γύρω από τρεις κύριες κατηγορίες: απειλές ταυτότητας, απειλές πρόσβασης και απειλές αποκάλυψης. Οι απειλές οργανώνονται κατά διάφορα είδη όπως η κακή χρήση των ταυτοτήτων των ασθενών, η μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση Προσωπικών Δεδομένων Υγείας (ΠΔΥ) ή η αποκάλυψη ΠΔΥ. Κάθε κατηγορία θεωρεί τρεις τύπους ‘εχθρών’: ο ίδιος ο ασθενής, τα μέλη (εξουσιοδοτημένοι χρήστες σε ΠΔΥ, προσωπικό του οργανισμού ΠΔΥ ή προσωπικό άλλου κινητού συστήματος υποστήριξης υγείας), και τέλος τα τρίτα μέλη (τρίτα μέλη που ενεργούν χωρίς εξουσιοδότηση).

Μια άλλη μελέτη αναφέρει ότι οι περισσότεροι άνθρωποι είναι εξοικειωμένοι με κοινούς τύπους παραβιάσεων της ασφάλειας που προκαλούνται από ιούς υπολογιστών, το Διαδίκτυο, χάκερ, σκουλήκια και κακόβουλο λογισμικό, με σκοπό να θέσουν σε κίνδυνο ή να διαταράξουν άλλα συστήματα ηλεκτρονικών υπολογιστών, καθώς και με την απώλεια ή κλοπή φορητών υπολογιστών που περιέχουν ευαίσθητα δεδομένα. Η ασφάλεια υπολογιστών ενσωματωμένη σε εξελιγμένες ιατρικές συσκευές και η μη εξουσιοδοτημένη επικοινωνία μπορεί να αυξήσει την ευαισθησία σε παραβιάσεις της ασφάλειας. Ο πίνακας 4.2 συνοψίζει τις μελέτες που έχουν γίνει για τον προσδιορισμό απειλών σε ΠΣΥ. Συνολικά, τριάντα απειλές είχαν ταξινομηθεί. Σημειώνεται ότι « οι σκόπιμες πράξεις κλοπής δεδομένων", "η κακή χρήση των πόρων του συστήματος", "τα λάθη των χρηστών", "οι αποκλίσεις στην ποιότητα των παρεχόμενων υπηρεσιών" είναι μεταξύ των κοινών απειλών για τα ΠΣΥ.

Πίνακας 4.2 *Σύνοψη μελετών που έχουν γίνει για τον προσδιορισμό απειλών σε ΠΣΥ*

Threats to HIS	Samy (2011)	Pardue (2011)	Sharma (2011)	Kohno (2010)	Whitman (2009)	Summer (2009)	Caballero (2009)	Richardson (2008)	Ilias (2006)	Whitman (2003)	Power (2002)	Rindfleisch (1997)	Loch (1992)
Power Failure/loss	√						√		√				
Network Infrastructure Failures or Errors	√						√	√	√		√		
Technological Obsolescence	√				√					√			
Hardware Failures or Errors	√	√			√		√		√	√			
Software Failures or Errors	√	√			√	√	√		√	√			
Operational Issues	√								√				
Communications Interception	√										√		
Repudiation	√												
Espionage or Trespass	√						√						
Communications Infiltration	√							√	√		√		
Social Engineering Attacks	√												
Technical Failure	√												
Deliberate Acts of Theft of Data	√		√		√		√	√	√	√	√		
Misuse of System Resources	√		√		√		√		√	√	√	√	√
Unauthorized Communication				√				√			√		
Staff Shortage	√								√				
User Errors	√	√	√		√	√	√	√	√	√		√	√
Sabotage or Willful Damages	√				√	√	√		√	√			
Environmental Threats	√						√		√				√
Deviations in Quality of Service	√	√	√	√	√	√	√	√		√	√	√	√
Maintenance Error									√				
Misuse of Web Application	√							√	√				
Compromises to Intellectual Property					√					√			
Missing, Inadequate or Incomplete Organizational Policy or Planning			√		√								√
Missing, Inadequate or Incomplete Controls			√		√							√	√
Financial Fraud							√	√			√	√	
Terrorism	√												
Unauthorized Access to Information Database		√	√					√			√	√	√
Natural Disasters		√	√		√		√	√	√	√			√
Theft of Equipment	√		√	√	√		√	√		√	√		

Προκειμένου να προστατευθούν οι πληροφορίες στην οργανισμό, αρχικά, προτείνεται να αναγνωριστούν τα συστήματα προστασίας και αποθήκευσης δεδομένων, μετάδοσης και επεξεργασίας. Δεύτερον, θα πρέπει να αντιμετωπιστούν οι ταξινομημένες απειλές. Έτσι, το προσωπικό της ασφάλειας πληροφοριών πρέπει να ενημερώνεται σχετικά με τις διάφορες απειλές στα περιουσιακά στοιχεία των πληροφοριακών συστημάτων. Όσον αφορά το ΠΣΥ, υπάρχουν έξι προτεινόμενες συνιστώσες οι οποίες περιλαμβάνουν το λογισμικό, το υλικό, τα δεδομένα, τους ανθρώπους, τις διαδικασίες και τα δίκτυα. Αυτές οι κρίσιμες συνιστώσες

επιτρέπουν στις πληροφορίες να εισαχθούν, να υποβληθούν σε επεξεργασία, να παραχθούν και να αποθηκευθούν. Κάθε μια από αυτές τις συνιστώσες έχει ορισμένα πλεονεκτήματα και αδυναμίες, καθώς και χαρακτηριστικά και χρήση. Κάθε συνιστώσα του ΠΣ έχει επίσης τις δικές της απαιτήσεις ασφάλειας. Συνεπώς, απαιτείται μια οργανωμένη ταξινόμηση των απειλών προκειμένου να συζητηθούν ζητήματα ασφάλειας των πληροφοριών.

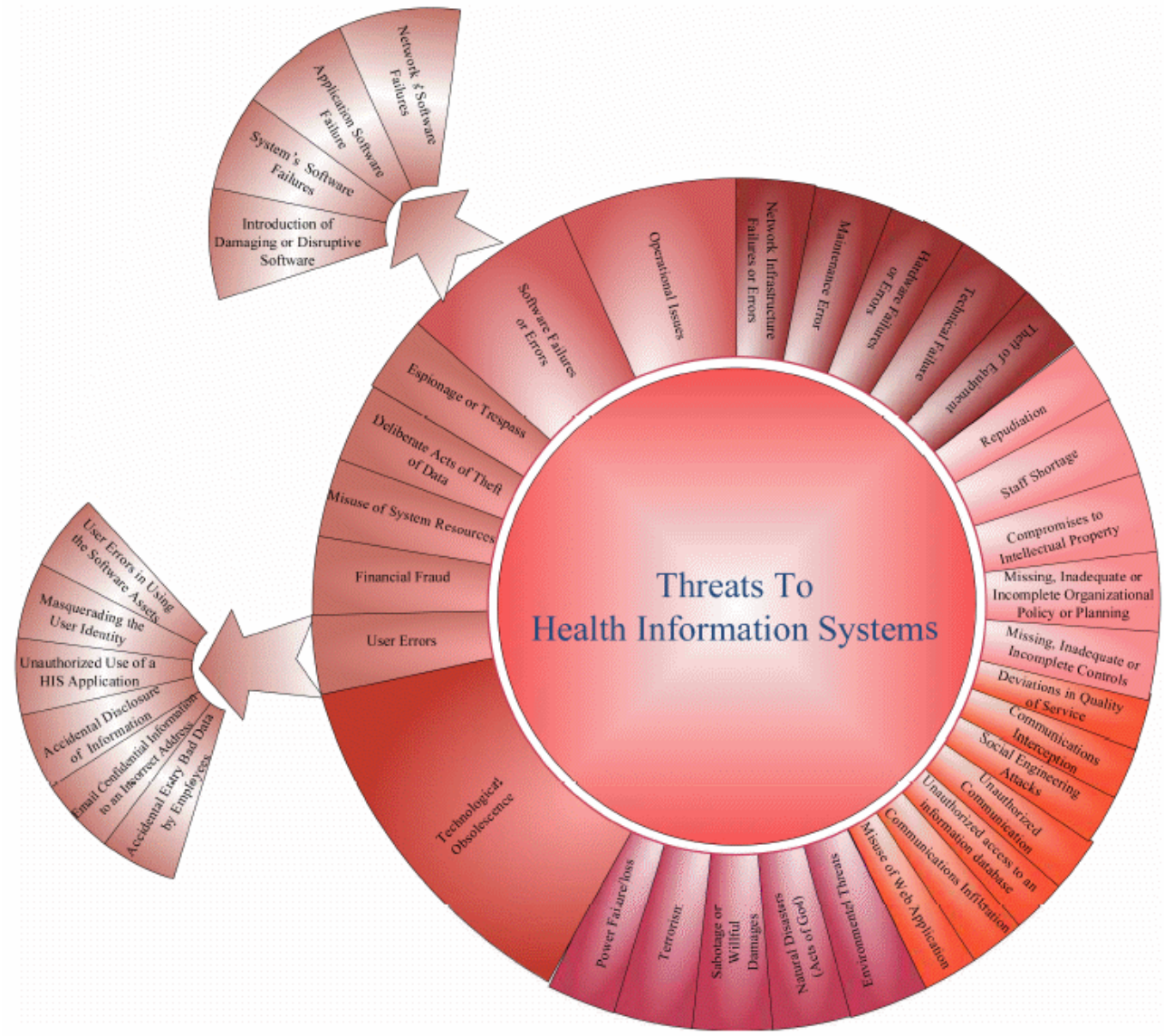
Παρακάτω παρουσιάζεται μια δομή δένδρου για την καταγραφή απειλών στα περιουσιακά στοιχειά υγειονομικής περίθαλψης ως ένα δένδρο απειλών. Ο σκοπός του δένδρου απειλών που παρουσιάζεται εδώ είναι να διευκολυνθεί η εκτίμηση κινδύνων και η παροχή πολιτικής και νομοθεσίας υγειονομικής περίθαλψης με την χρησιμοποίηση δευτερογενών πόρων δεδομένων όπως απεικονίζονται στον πίνακα 4.3. ο κατάλογος απειλών πληροφοριών υγείας έχει θετικά αποτελέσματα στην εκτίμηση κινδύνου και χρειάζεται την κατηγοριοποίηση και την τεκμηρίωση περισσότερο από ό,τι φαίνεται απλώς στον πίνακα 4.3. Η εκτίμηση του κινδύνου πρέπει να παρέχει τις διάφορες πηγές απειλών σε ΠΣΥ.

Πίνακας 4.3 *Δέντρο απειλών για ΠΣΥ*

1. Power Failure/loss	19. Sabotage or Willful Damages
1.1 Power Failure of Server	20. Natural Disasters (Acts of God)
1.2 Power Failure of Workstation	20.1 Flood
2. Network Infrastructure Failures or Errors	20.2 Landslides
2.1Technical Failure of Network Interface	20.3 Earthquake
2.2 Technical Failure of Network Services	20.4 Electrical storms
2.3 Abuse of Wireless Network	20.5 Lightning
3. Technological Obsolescence	20.6 Tornadoes
4. Hardware Failures or Errors	20.7 Avalanches
4.1 System's Hardware Failures	21. Environmental Threats
4.2 Switch	21.1 Water Damage
4.3 Hub	21.2 Fire
4.4 Router	21.3 Air-condition Failure
4.5 Server	21.4 Pollution
4.6 Firewall	21.5 Chemicals
4.7 Others	21.6 Liquid Leakage
4.8 Network's Hardware Failures	22. Deviations in Quality of Service
5. Software Failures or Errors	22.1 QoS Deviations from Service Providers
5.1 Introduction of Damaging or Disruptive Software	22.2 Deliberate Software Attacks
5.2 System's Software Failures	22.2.1 Nonetheless Purposeful, attempt to circumvent system security
5.3 Network's Software Failures	22.2.2 Malicious Attempt to gain unauthorized access
5.4 Bugs	22.2.2.1 Password Sniffing
5.5 Code Problems	22.2.2.2 Telecom Eavesdropping
5.6 Unknown Loopholes	22.2.2.3 Database Attack
6. Operational Issues	22.2.2.4 Denial of Service
7. Communications Interception	22.2.2.5 Web Site Defacement

8. Repudiation	22.2.2.6 Bots
9. Espionage or Trespass	22.2.2.7 DNS Attacks
10. Communications Infiltration	22.2.2.8 Malware Attack
10.1 Device Reprogramming	22.2.2.8.1 Worm
10.2 Unauthorized Data Extraction	22.2.2.8.2 Trojan Horses
11. Social Engineering Attacks	22.2.2.8.3 Spyware
12. Technical Failure	22.2.2.8.4 Virus
13. Deliberate Acts of Theft Data	22.2.2.8.5 Adware
13.1 Theft/loss of Customer Data or Proprietary Info	22.2.2.8.6 Macros
13.2 Illegal Confiscation of Equipment or Information	23. Maintenance Error
13.3 Dumping Physical Files with Critical Information in Public	23.1 Hardware
14. Misuse of System Resources	23.2 Software
14.1 Third Party	23.3 Network
14.2 Information Extortion	24. Misuse of Web Application
15. Unauthorized Communication	24.1 Cross Site Scripts
16. Unauthorized Access to Information Database	24.2 Information Leakage
17. Staff Shortage	24.3 SQL Injection
18. User Errors	24.4 HTTP Response Splitting
18.1 User Errors in Using the Software Assets	25. Compromises to Intellectual Property
18.2 Masquerading the User Identity	26. Missing, Inadequate or Incomplete Organizational Policy or Planning
18.3 Unauthorized Use of a HIS Application	27. Missing, Inadequate or Incomplete Controls
18.4 Accidental Disclosure of Information	28. Financial Fraud
18.5 Email Confidential Information to an Incorrect Address	29. Terrorism
18.6 Accidental Entry Bad Data by Employees	30. Theft of Equipment

Κάθε μια από τις απειλές στο δέντρο χρησιμοποιείται για την παροχή ενός συνόλου ελέγχων ώστε να μειωθεί ο κίνδυνος εκμετάλλευσης των ευπαθειών. Από τον πίνακα 4.3, μπορούμε να παρουσιάσουμε την κατηγοριοποίηση σε μορφή πίτας για καλύτερη απεικόνιση και κατανόηση. Το Σχήμα 4.3, επίσης, δείχνει εμφανώς μια απλή εικόνα των απειλών σε ΠΣΥ.



Σχήμα 4.3 *Απλό μοντέλο του δέντρου απειλών για ΠΣΥ*

Συνοψίζοντας, τα ΠΣΥ θα μπορούσαν να υποβληθούν σε απειλές ασφάλειας από μια ή περισσότερες πηγές συμπεριλαμβανομένων των απατηλών παραγόντων, της μη εξουσιοδοτημένης χρήσης των πόρων, της μη εξουσιοδοτημένης αποκάλυψης των πληροφοριών, της αλλοίωσης των πόρων και της μη εξουσιοδοτημένης άρνησης υπηρεσιών (Win et al. 2006). Οι επιθέσεις άρνησης υπηρεσιών (DoS) μέσω σκουληκιών ή ιών Διαδικτύου, οι δυσλειτουργίες εξοπλισμού που προκύπτουν από την διαγραφή αρχείων ή την αλλοίωση δεδομένων, και η έλλειψη σχεδίων έκτατης ανάγκης, οι διαδικασίες αποκατάστασης δεδομένων, καθώς και παρόμοιες δραστηριότητες μπορούν επίσης να προκαλέσουν παραβιάσεις της νομοθεσίας HIPPA (Mercuri 2004).

4.6 Συμπεράσματα

Η εξέλιξη στον τομέα της υγείας προς μια κοινότητα εξαρτώμενη από την Τεχνολογία της Πληροφορικής (Information Technology-IT), είναι αναμφισβήτητα μια πρόκληση όσον αφορά την ασφάλεια και την ιδιωτικότητα. Η πρόοδος στον τομέα της Τεχνολογίας της Πληροφορικής και η υιοθέτησή της από τον τομέα της υγείας είναι πιθανόν να βελτιώσει την ποιότητα παροχής υγειονομικής περίθαλψης, να μειώσει το κόστος της και να εξελίξει την ιατρική επιστήμη. Ωστόσο, ο μετασχηματισμός αυτός έχει αυξήσει τη δυνατότητα κινδύνων κατά της ασφάλειας πληροφοριών και την δυνατότητα παραβίασης της ιδιωτικότητας. Επιπλέον, με την αυξανόμενη ψηφιοποίηση των αρχείων υγείας, η παραβίαση ιατρικών δεδομένων έχει καταστεί ως το πλέον απειλητικό ζήτημα για τους ασθενείς. Ανεκδοτικά στοιχεία δείχνουν ότι οι πιο σημαντικές απειλές για την ιδιωτικότητα του ασθενή προέρχονται από εσωτερικούς παράγοντες, όχι εξωτερικούς.

Έχοντας εξετάσει περιληπτικά τις τωρινές τάσεις και τα κρίσιμα ζητήματα ασφάλειας που αφορούν τα ΠΣΥ, είναι προφανές ότι, η μελέτη των προβλημάτων που συνδέονται με την προστασία των δεδομένων και την ασφάλεια των ΠΣΥ δεν επαρκεί για την άμεση λύση των ενδεχόμενων διλλημάτων, εμποδίων και δυσλειτουργιών που τα αφορούν. Επομένως, θα πρέπει να γίνεται μια συνεχής προσπάθεια για την αναζήτηση και συμπλήρωση νέων λύσεων.

Κεφάλαιο 5

Πρακτική Εφαρμογή Ανάλυσης Κινδύνων στη Διαλειτουργικότητα ΠΣΥ με χρήση της μεθόδου CRAMM

5.1 Εισαγωγή

Η διαχείριση κινδύνων, ως αρχή, δεν είναι πλέον ένα απλό ζήτημα εκτίμησης χαρτοφυλακίου. Είναι επιτακτική η ανάγκη, τα διάφορα ιδρύματα να τυποποιούν και να διαχειρίζονται τους κινδύνους της Τεχνολογίας Πληροφοριών (ΤΠ) σε ένα αποδεκτό επίπεδο, έτσι ώστε η συχνότητα και το μέγεθος των αρνητικών επιπτώσεων να μην παρεμποδίζουν σε σοβαρό βαθμό την αποστολή του ιδρύματος.

Η διαχείριση κινδύνων, έως τώρα, εφαρμόζεται στον τομέα Νοσοκομειακών Πληροφορικών Συστημάτων (ΝΠΣ) αφού το δευτεροβάθμιο επίπεδο φροντίδας υγειονομικής περίθαλψης έχει τα περισσότερα Πληροφοριακά Συστήματα (ΠΣ) σε ισχύ. Η διαχείριση κινδύνων στα Περιφερειακά Δίκτυα Υγείας (ΠΔΥ) είναι μια πιο περίπλοκη διαδικασία καθώς τα Πληροφοριακά Συστήματα ΠΔΥ απαρτίζονται από ΠΣ πολλαπλών οργανισμών και εξαρτώνται κυρίως από την διαλειτουργικότητα των υφιστάμενων και νέων ΠΣ.

Στο κεφάλαιο αυτό, η ανάλυση κινδύνων θα βασιστεί κυρίως στις τεχνολογικές απειλές που αφορούν ένα περιφερειακό περιβάλλον. Γίνεται όμως και μια επίκληση σε απειλές που αφορούν τις φυσικές καταστροφές, το φυσικό και θεσμικό περιβάλλον, τον ανθρώπινο παράγοντα και τις επιχειρησιακές απειλές. Στην περιπτωσιολογική μελέτη παρουσιάζεται η διαδικασία εκτίμησης κινδύνων σε μια υποτιθέμενη Περιφερειακή Αρχή Υγείας (ΠΑΥ). Το περιβάλλον της εν λόγω Αρχής περιλαμβάνει ποικίλα ΠΣ που πρέπει να ενσωματωθούν μέσω μηχανισμών ενδιάμεσου λογισμικού (middleware), προκειμένου να υποστηρίξουν ποιοτικές υπηρεσίες υγείας.

Για την πραγματοποίηση της ανάλυσης χρησιμοποιείται η μέθοδος CRAMM που δημιουργήθηκε από την Υπηρεσία ασφαλείας της Βρετανική κυβέρνησης. Η μέθοδος αυτή βασίζεται στην ποιοτική (qualitative) ανάλυση κινδύνων, όπου ο υπολογισμός της πιθανότητας να συμβεί μια απειλή και της αξίας των περιουσιακών στοιχείων δεν είναι απόλυτος όπως στις μεθόδους ποσοτικών (quantitative) αναλύσεων, αλλά βασίζεται σε προκαθορισμένες κλίμακες. Το πλεονέκτημα είναι η ελαχιστοποίηση του χρόνου της ανάλυσης χωρίς να επιβαρύνεται ιδιαίτερα η ακρίβεια των αποτελεσμάτων.

Τέλος, από την ανάλυση αυτή, είναι σαφές ότι η αποτελεσματική χαρτογράφηση δεδομένων και των συσχετιζόμενων διαδικασιών αποτελεί κρίσιμο παράγοντα επιτυχίας στην εφαρμογή μιας τέτοιας σύνθετης μελέτης, όπως η εφαρμογή ενός Περιφερειακού ΠΣΥ (ΠΠΣΥ).

5.2 Επεξήγηση της μεθόδου CRAMM

Η μέθοδος CRAMM, όπως έχει ήδη αναφερθεί σε προηγούμενο κεφάλαιο, βασίζεται στην αναγνώριση και αξιολόγηση των περιουσιακών στοιχείων (assets) του οργανισμού, στην αναγνώριση και αξιολόγηση των απειλών που υπάρχουν προς αυτά, καθώς και την ευπάθεια τους προς τις συγκεκριμένες απειλές. Ο συνδυασμός αξίας – απειλών – ευπαθειών επιτρέπει τον υπολογισμό του βαθμού του κινδύνου (risk) που διατρέχει κάθε περιουσιακό στοιχείο προς κάθε συγκεκριμένη απειλή, με βάση μια κλίμακα κινδύνου. Με τον υπολογισμό αυτό φαίνεται τι κινδυνεύει και με ποιο τρόπο, ώστε να μπορούμε να υιοθετήσουμε σωστούς και οικονομικούς (cost effective) τρόπους αντιμετώπισης. Επιπρόσθετα, η χρήση της κλίμακας του κινδύνου επιτρέπει τον προσδιορισμό προτεραιοτήτων στην υλοποίηση των αντιμέτρων.

Συγκεκριμένα, η μέθοδος CRAMM οργανώνεται σε τρία βασικά στάδια. Αρχικά, τα περιουσιακά στοιχεία του συστήματος προσδιορίζονται και ταξινομούνται ως δεδομένα, προγράμματα εφαρμογών και υλικά περιουσιακά στοιχεία (εξοπλισμός, κτήρια, προσωπικό). Τα περιουσιακά στοιχεία δεδομένων αποτιμώνται από την άποψη των επιδράσεών τους σε παραβιάσεις εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και μη αποποίησης, που είναι οι ευρέως αποδεκτές αρχές της ασφάλειας πληροφοριών. Τα υλικά περιουσιακά στοιχεία και εκείνα των εφαρμογών αποτιμώνται όσον αφορά την μη διαθεσιμότητα, την αντικατάσταση ή την αναπροσαρμογή του κόστους τους. Οι πιθανές απειλές και οι γνωστές ευπάθειες ποσοτικοποιούνται κατά επιλεγμένες ομάδες περιουσιακών στοιχείων, ενώ η πιθανότητα εμφάνισής τους υπολογίζεται χρησιμοποιώντας προκαθορισμένα επίπεδα απειλών και ευπαθειών (πχ “Very Low”, “Low”, “Medium”, “High”, “Very High”). Τέλος, για την διαχείριση των εντοπιζόμενων κινδύνων, παράγεται ένα σύνολο από αντίμετρα που εφαρμόζονται στο ΠΣ.

Συνοψίζοντας, η μέθοδος CRAMM αποτελείται από τα εξής στάδια:

- Αναγνώριση των περιουσιακών στοιχείων
- Δημιουργία ενός μοντέλου συσχέτισης μεταξύ τους
- Αξιολόγηση των περιουσιακών στοιχείων
- Αναγνώριση των απειλών προς τα περιουσιακά στοιχεία
- Αξιολόγηση της πιθανότητας να συμβεί μια απειλή καθώς και της ευπάθειας του κάθε περιουσιακού στοιχείου προς την απειλή αυτή
- Υπολογισμός του βαθμού κινδύνου

- Υπολογισμός των πιθανών αντιμέτρων

Κάθε ένα από τα παραπάνω βήματα θα αναλυθούν παρακάτω σε συνδυασμό με τα αποτελέσματα από την ανάλυση στο ΠΔΥ.

5.3 Προσδιορισμός Γενικού Πλαισίου

Πολυάριθμες αναφορές που έχουν δημοσιευθεί τα τελευταία χρόνια δείχνουν ότι οι αυτοματοποιημένες λειτουργίες και τα ηλεκτρονικά δεδομένα δεν προστατεύονται επαρκώς. Οι αναφορές αυτές δείχνουν ότι ο κακός σχεδιασμός της διαχείρισης της ασφάλειας είναι ένα από τα σημαντικότερα υποκείμενα προβλήματα. Η κύρια πρόκληση που αντιμετωπίζουν πολλές αρχές είναι στην αναγνώριση και ταξινόμηση των κινδύνων ενάντια της ασφάλειας πληροφοριών στις λειτουργίες τους, που είναι το πρώτο βήμα στην ανάπτυξη και διαχείριση ενός αποτελεσματικού προγράμματος ασφάλειας. Η λήψη του μέτρου αυτού, βοηθά στο να διασφαλιστεί ότι οι οργανισμοί εντοπίζουν τους πιο σημαντικούς κινδύνους και καθορίζει ποιες ενέργειες είναι κατάλληλες για το μετριασμό τους.

Ένα Περιφερειακό Δίκτυο Υγείας (ΠΔΥ) μπορεί να θεωρηθεί ως ένα ενδο-οργανωτικό περιφερειακό σύστημα που βασίζεται σε μια Περιφερειακή Αρχή Υγείας (ΠΑΥ). Η ΠΑΥ υποστηρίζεται από οργανωτικές ρυθμίσεις προκειμένου να διαχειριστεί και να ενσωματώσει τη ροή πληροφοριών για υπηρεσίες υγείας, με απώτερο σκοπό την βελτίωση της εξυπηρέτησης πελατών και την βελτίωση της οργανωτικής αποτελεσματικότητας σε θέματα υγειονομικής φύσεως.

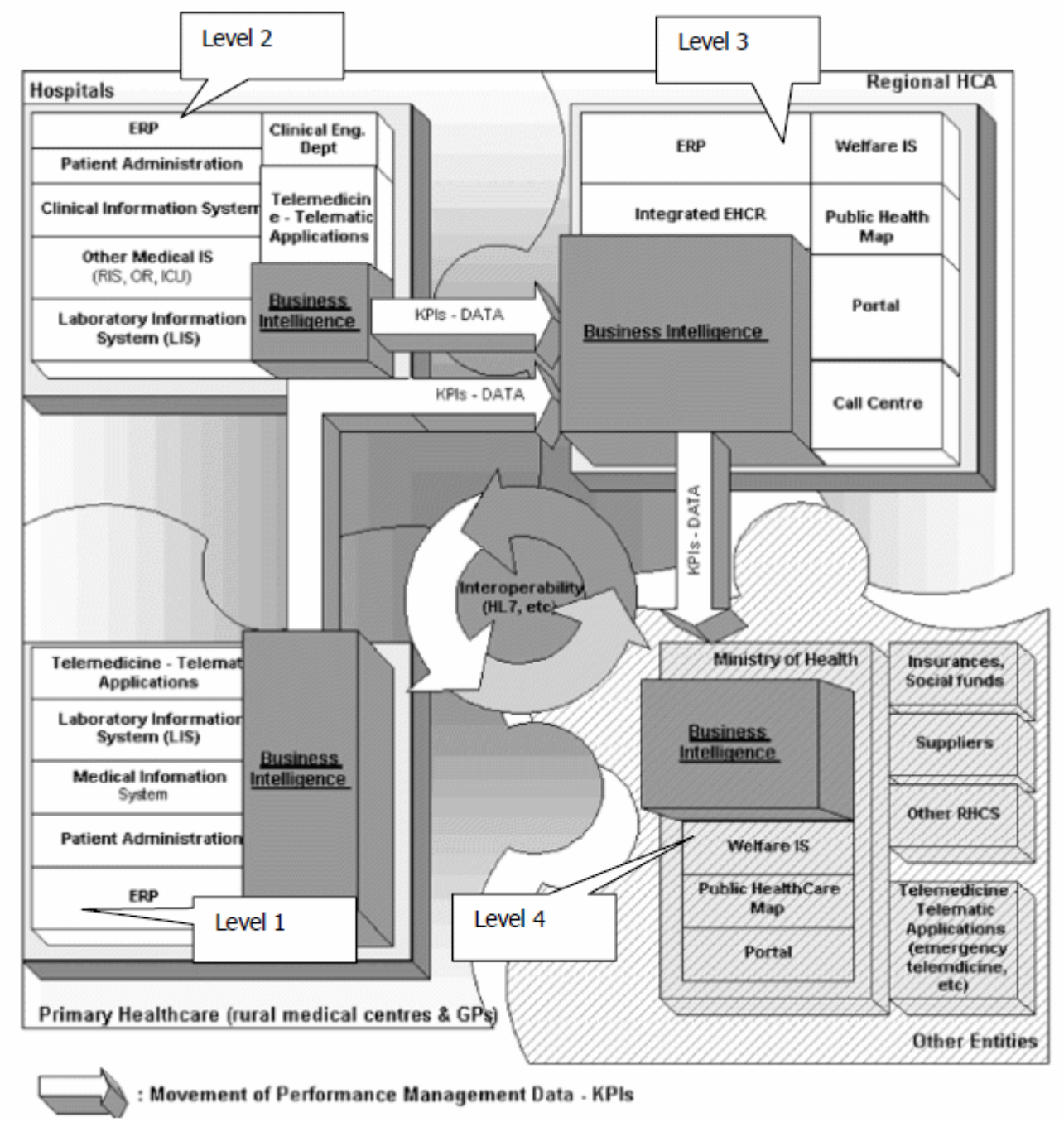
Μερικές από τις υπηρεσίες που παρέχονται από ένα ΠΔΥ είναι οι ακόλουθες:

- Καθημερινή επικοινωνία για συνταγογράφηση φαρμάκων, αναφορές, εργαστηριακά αποτελέσματα κτλ.
- Ασφάλεια ηλεκτρονικού ταχυδρομείου για πληροφορίες σχετικές με τον ασθενή
- Κράτηση εγκαταστάσεων για την φύλαξη νοσοκομειακών και διαγνωστικών πληροφοριών
- Ιατρικά αρχεία κοινής χρήσης
- Συστήματα έκτακτης ανάγκης και συναγερμού
- Εγκαταστάσεις τηλε-ιατρικής
- Πρωτόκολλα και κατευθυντήριες οδηγίες για διατομεακή θεραπεία
- Ιστοσελίδες πληροφοριών υγείας για τους επαγγελματίες, ασθενείς και το κοινό
- Διοικητικού χαρακτήρα διατομεακά πληροφοριακά συστήματα και συστήματα διαχείρισης

Ένα ΠΔΥ ακολουθεί μηχανισμούς τεσσάρων επιπέδων για την λήψη αποφάσεων και την διαχείριση της απόδοσης. Τα τέσσερα αυτά επίπεδα περιλαμβάνουν:

- Επίπεδο 1: Ο Πρωτογενής τομέας υγείας
- Επίπεδο 2: Τα Νοσοκομεία
- Επίπεδο 3: Η Περιφερειακή Αρχή Υγείας (ΠΑΥ)
- Επίπεδο 4: Το Υπουργείο Υγείας

Οι συνιστώσες του κάθε επιπέδου φαίνονται στο Σχήμα 5.1. Επιπλέον, η ανάλυση τεσσάρων επιπέδων αναφέρεται γενικά σε κάθε ίδρυμα υγειονομικής περίθαλψης (ιδιωτικό ή δημόσιο), σε εθνικό επίπεδο για κάθε χώρα, στα πλαίσια της βελτίωσης της εξυπηρέτησης ασθενών, όπως απεικονίζεται στο Σχήμα 5.1.



Σχήμα 5.1 *Συνιστώσες που απαρτίζουν ένα ΠΔΥ*

Η ενσωμάτωση ετερογενών ΠΣ που υποστηρίζουν τις συνιστώσες των Περιφερειακών Δικτύων Υγείας, εξασφαλίζοντας ταυτόχρονα την ροή δεδομένων σε ασφαλή περιβάλλοντα, είναι μια νέα πρόκληση. Δεδομένου ότι η Τεχνολογία Πληροφοριών έχει διεισδύσει ως επί το πλείστον στα νοσοκομεία (επίπεδο 2), υπάρχει τώρα η ανάγκη να ενσωματωθούν τα ετερογενή Νοσοκομειακά Πληροφοριακά Συστήματα (ΝΠΣ), υπό την αιγίδα του Συστήματος Περιφερειακού Πληροφοριακού Δικτύου Υγείας (επίπεδο 3) (Regional Healthcare Network Information System). Η ενσωμάτωση σε τεχνολογικό επίπεδο μπορεί να εφαρμοστεί με την εκμετάλλευση Συστημάτων Διαχείρισης Ροής Εργασιών (Workflow Management Systems) και την εκμετάλλευση προσανατολισμένων σε μηνύματα μηχανισμών ενδιάμεσου λογισμικού (Message Oriented Middleware).

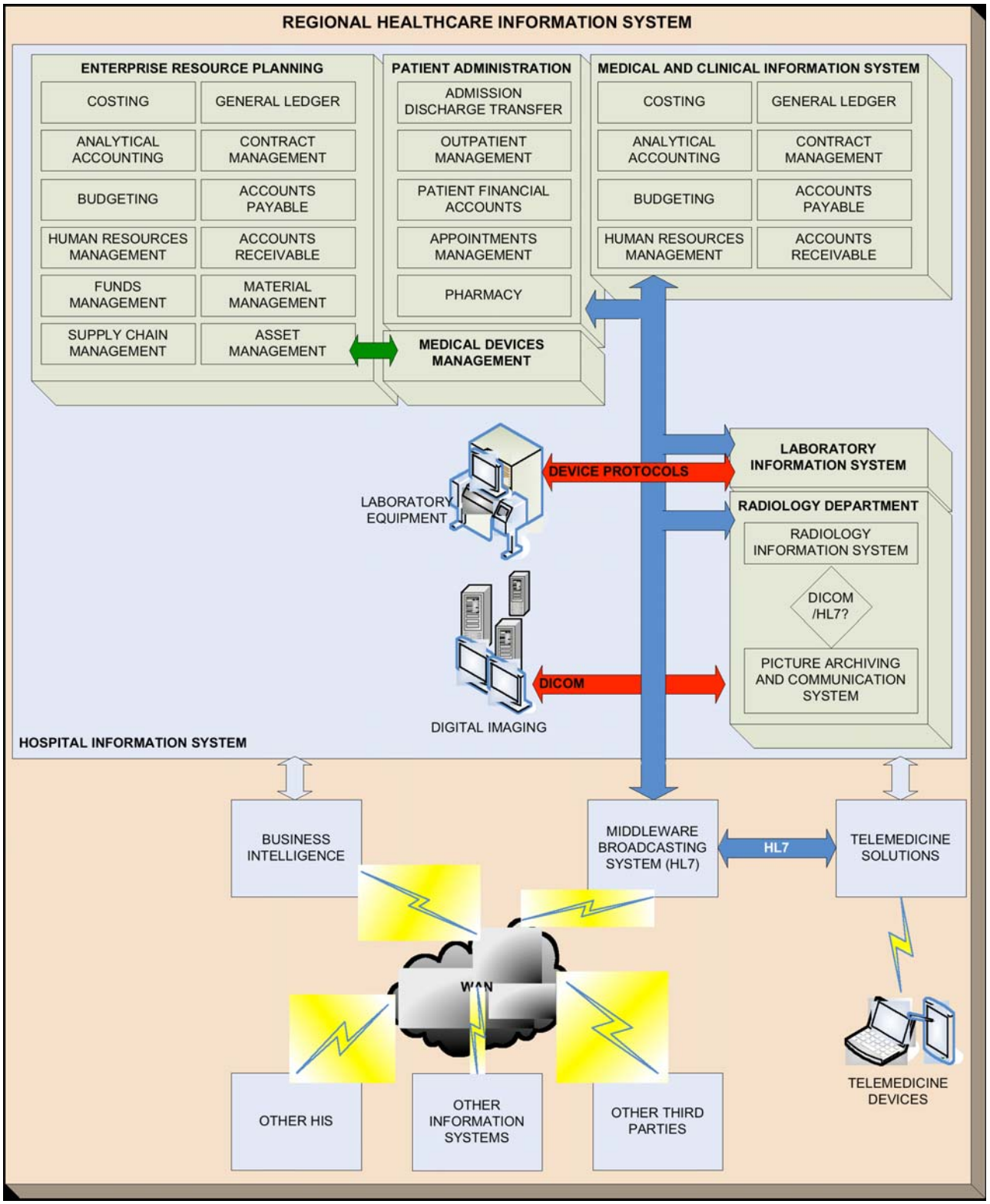
Όσον αφορά τα προαναφερθέντα, έχει προκύψει η ανάγκη συνεργασίας των ΠΣΥ ως συνιστώσες των ΠΔΥ, όπου τα νέα ΠΣ πρέπει να επικοινωνούν με ήδη υπάρχοντα συστήματα σε διάφορα ιδρύματα υγειονομικής περίθαλψης. Μια προτεινόμενη λύση είναι η χρήση συστημάτων αναμετάδοσης ενδιάμεσου λογισμικού (middleware broadcasting systems), που είναι βασισμένα στην ανταλλαγή πληροφοριών μέσω μηνυμάτων χρησιμοποιώντας κάποιο πρωτόκολλο εφαρμογής (ISO- επίπεδο 7 του OSI) κάτω από το πρότυπο του HL7. Για την επίτευξη επικοινωνίας μεταξύ νέων και παλαιών συστημάτων, όλα τα συστήματα είναι συνδεδεμένα, μέσω μιας ενιαίας διεπαφής, σε ένα πλαίσιο διαλειτουργικότητας ή ακόμα πιο τεχνικά σε μια Κοινή Υποδομή Επικοινωνίας (ΚΥΕ) (Common Communication Infrastructure-CCI).

Με τη χρήση αυτού του είδους διαλειτουργικότητας, νέες διαδικασίες και ροές δεδομένων πρέπει να εισαχθούν στις υφιστάμενες διαδικασίες της κάθε μονάδας υγείας. Επομένως, είναι σαφές ότι απαιτείται μια εκτίμηση κινδύνου που να απεικονίζει όλα τα θέματα ασφάλειας, να αναγνωριστούν οι απειλές και να προταθούν συγκεκριμένα αντίμετρα. Έτσι, γίνεται μια προσπάθεια με απώτερο σκοπό να εφαρμοστεί ένας ολοκληρωμένος εικονικός οργανισμός υγείας, ιδιαίτερα σε περιφερειακό επίπεδο, για την εναρμόνιση διαδικασιών και πληροφοριών μεταξύ των επικοινωνούντων φορέων υγειονομικής περίθαλψης (μέσω των πληροφοριακών συστημάτων τους).

Η ολοκλήρωση σε αυτό το περιβάλλον πολλαπλών οργανισμών θα μπορούσε να εφαρμοστεί μόνο σε ένα ασφαλές περιβάλλον. Η ασφάλεια περιλαμβάνει διοικητικά, φυσικά και τεχνικά μέτρα για να εξασφαλιστεί η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα των δεδομένων και των ΠΣ. Η ασφάλεια αφορά την ασφαλή επικοινωνία, που αποτελείται από ασφαλή συνδεσιμότητα και ασφαλή μεταφορά μηνυμάτων καθώς επίσης και την ασφαλή συνεργασία κατανεμημένων συστημάτων που βασίζονται σε δίκτυα ή την ασφάλεια εφαρμογών. Το επίπεδο πολυπλοκότητας των πτυχών της ασφάλειας στον τομέα της υγείας εξαρτάται από το επίπεδο του παρόχου υγειονομικής περίθαλψης σύμφωνα με την τεσσάρων επιπέδων

ιεραρχία που απεικονίζεται στο Σχήμα 5.1. Ο βασικός τομέας είναι η πρωτογενής μονάδα φροντίδας. Όσο υψηλότερο το επίπεδο παροχής υπηρεσιών υγείας, ήτοι περιφερειακό ή εθνικό επίπεδο, τόσο πιο σύνθετες γίνονται και οι πτυχές της ασφάλειας. Ο κρισιμότερος παράγοντας σε αυτά τα επίπεδα είναι η ανάγκη διαλειτουργικότητας μεταξύ των διαφόρων οργανισμών υγείας. Μια εθνική πολιτική ασφάλειας για την αξιοποίηση της ΤΠ&Ε χρησιμοποιείται σε χώρες της ΕΕ. Παρόλα αυτά, λίγες χώρες έχουν μια εθνική πολιτική ασφάλειας για την υγειονομική περίθαλψη. Παρακάτω παρουσιάζεται η διαχείριση κινδύνων σε ασφαλή κρίσιμα περιβάλλοντα, ώστε να εξασφαλιστεί η ολοκλήρωση και η συνοχή δεδομένων και διαδικασιών σε δια-οργανωτικά περιβάλλοντα.

Η διαχείριση κινδύνων εφαρμόζεται μέχρι στιγμής στον τομέα ΝΠΣ αφού το δεύτερο επίπεδο υγειονομικής περίθαλψης έχει τα περισσότερα ΠΣ σε ισχύ. Όπως έχει ήδη αναφερθεί, η διαχείριση κινδύνων στα Περιφερειακά Δίκτυα Υγείας (ΠΔΥ) είναι μια πιο περίπλοκη διαδικασία καθώς τα Πληροφοριακά Συστήματα ΠΔΥ απαρτίζονται από ΠΣ πολλαπλών οργανισμών και εξαρτώνται κυρίως από την διαλειτουργικότητα υφιστάμενων και νέων ΠΣ. Στο Σχήμα 5.2 παρουσιάζεται η πολυπλοκότητα ενός Περιφερειακού Πληροφοριακού Συστήματος Υγείας (ΠΠΣΥ).



Σχήμα 5.2 *Περιφερειακό πληροφοριακό σύστημα υγείας (ΠΠΣΥ)*

Ο προσδιορισμός πλαισίου είναι μια περίπλοκη διαδικασία για ένα περιβάλλον πολλαπλών οργανισμών. Έμφαση δίνεται στις απαιτήσεις ασφάλειας των μονάδων υγείας (σε όλα τα

επίπεδα) και ως επί τω πλείστων στη διασύνδεση μεταξύ οργανισμών. Σε γενικές γραμμές το πλαίσιο/περιβάλλον των ΠΔΥ αποτελείται από τις ακόλουθες παραμέτρους:

- Δεδομένα του συστήματος
- Διαδικασίες
- Υποδομές ΤΠΕ του συστήματος (υλικό και λογισμικό)
- Διαλειτουργικότητα ΠΣ
- Οι χρήστες και οι ανθρώπινοι πόροι γενικότερα

Δεδομένου ότι η ολοκλήρωση ορίζεται σύμφωνα με:

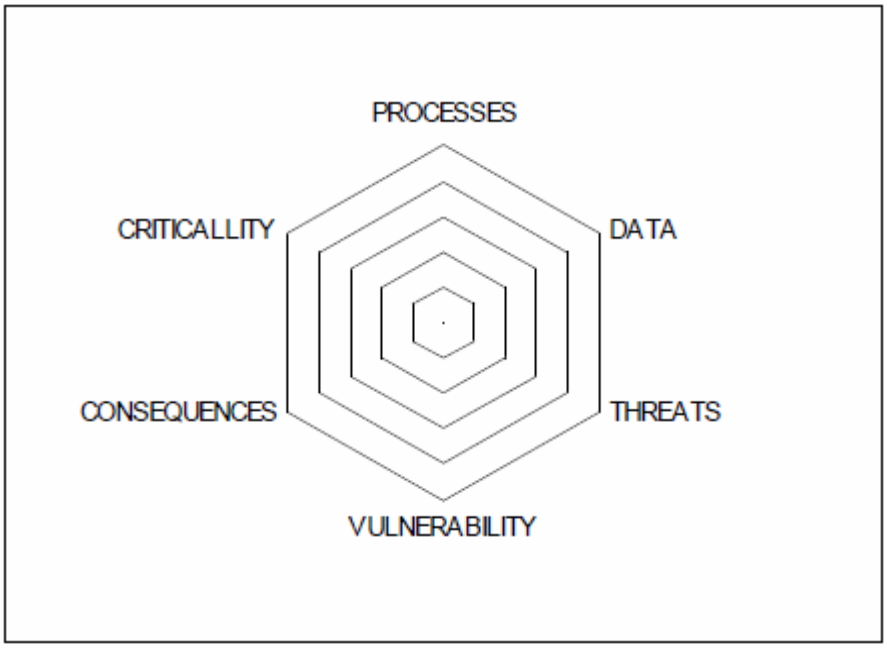
- την ολοκλήρωση δεδομένων από σημασιολογική άποψη
- την ολοκλήρωση συστημάτων από τεχνική άποψη
- την ολοκλήρωση διαδικασιών από σημασιολογική άποψη και
- την ολοκλήρωση παρουσίασης από τεχνική άποψη

πιστεύεται ότι η έμφαση της διαχείρισης κινδύνων θα πρέπει να δοθεί στα δεδομένα και τις διαδικασίες που χαρακτηρίζουν το σύστημα, χωρίς όμως να μειώνεται η σπουδαιότητα των υπόλοιπων ζητημάτων. Εντούτοις, είναι κοινό ότι τα σημαντικότερα ζητήματα δεν υποδηλώνουν συνήθως τα τεχνολογικά χαρακτηριστικά γνωρίσματα αλλά τα οργανωτικά. Πιο συγκεκριμένα, τα περιουσιακά στοιχεία δεδομένων είναι ανεξάρτητα από την αρχιτεκτονική του ΠΣ και του ΠΠΣΥ. Η ολοκλήρωση σε περιφερειακό επίπεδο εξαρτάται από στρατηγικές και την δυνατότητά τους να εφαρμοστούν και να καθιερωθούν επιτυχώς.

Τα δεδομένα που ανταλλάσσονται είναι τα σταθερά και έγκυρα περιουσιακά στοιχεία του συστήματος. Σε περιφερειακές ή εθνικές εφαρμογές για συστήματα υγείας πολλαπλών οργανισμών δίνονται διαφορετικές οδηγίες αρχιτεκτονικής. Δεδομένου ότι δεν υπάρχει μια έγκυρη πολιτική σε ισχύ, η διαχείριση κινδύνου και εν συνεχεία η πολιτική ασφάλειας θα πρέπει να σχεδιαστεί ανεξάρτητα από την αρχιτεκτονική. Αυτός είναι και ο λόγος που θεωρείται ότι η ολοκλήρωση υλοποιείται μέσω μηχανισμών ενδιάμεσου λογισμικού και πιο συγκεκριμένα μέσω της ασύγχρονης επικοινωνίας μηνυμάτων χρησιμοποιώντας, για παράδειγμα, το πρότυπο μηνυμάτων HL7.

Εντούτοις, το πλαίσιο στο περιφερειακό περιβάλλον υγείας είναι πολυδιάστατο. Αυτό απεικονίζεται σχηματικά στο Σχήμα 5.3. Η πιο σημαντική διάσταση είναι τα δεδομένα που ανταλλάσσονται στο σύστημα. Η δεύτερη διάσταση είναι οι διαδικασίες που υποστηρίζουν τις υπηρεσίες που παρέχονται από το σύστημα. Οι διαδικασίες θα πρέπει να καθορίζονται πριν από την εφαρμογή του συστήματος, κατά την φάση ανάλυσης. Η διαχείριση κινδύνου αφορά τις διαδικασίες που ενσωματώνουν διαφορετικά ΠΣ εντός του ΠΠΣΥ. Οι διαδικασίες και τα

δεδομένα, εν συνεχεία, εφαρμόζονται και υποστηρίζονται από τα δομικά στοιχεία του λογισμικού που είναι οι βασικές συνιστώσες του ΠΣ.



Σχήμα 5.3 *Το πολυδιάστατο πλαίσιο του συστήματος*

5.4 Εφαρμογή της Μεθόδου Ανάλυσης Κινδύνων

Η ανάλυση κινδύνων του ΠΠΣΥ έχει εκτελεστεί σύμφωνα με τις οδηγίες της μεθοδολογίας CRAMM. Το πρώτο στάδιο της ανάλυσης αποτελείται από την αναγνώριση και αποτίμηση των περιουσιακών στοιχείων του ΠΣ. Η αποτίμηση αφορά τα δεδομένα και τις κρίσιμες πληροφορίες που διαχειρίζονται από το σύστημα, καθώς και τις εφαρμογές υλικού και λογισμικού που χρησιμοποιούνται για την παροχή ιατρικών υπηρεσιών. Η κύρια προσέγγιση είναι να προσδιοριστούν, ως διακριτά περιουσιακά στοιχεία, όλες οι κατηγορίες δεδομένων που μπορούν να διαταράξουν την εξυπηρέτηση χρηστών, σε περίπτωση που διακυβεύεται η διαθεσιμότητα, η εμπιστευτικότητα ή η ακεραιότητά τους. Τα περιουσιακά στοιχεία υλικού και λογισμικού είναι εκείνα που συνδέονται με τις προαναφερθείσες κατηγορίες δεδομένων και ως εκ τούτου με την προσφερόμενη εξυπηρέτηση των χρηστών. Η αποτίμηση πραγματοποιήθηκε βάσει των πιθανών επιδράσεων που μια απειλή μπορεί να προκαλέσει στις απαιτήσεις παροχής ιατρικών υπηρεσιών από το ΠΠΣΥ.

5.4.1 Αναγνώριση και Αποτίμηση Περιουσιακών Στοιχείων

Τα περιουσιακά στοιχεία που αναλύονται με την μέθοδο CRAMM μπορούν να χωριστούν σε τέσσερις κατηγορίες:

- *Δεδομένα (Data assets):* Στην κατηγορία αυτή ανήκουν κάθε είδους δεδομένα, από δεδομένα προσωπικού χαρακτήρα σε μια βάση δεδομένων μέχρι και οι καταχωρήσεις σε έναν DNS εξυπηρετητή.
- *Υπηρεσίες (End User Services):* Στην κατηγορία αυτή ανήκουν οι υπηρεσίες που επιτρέπουν στον τελικό χρήστη πρόσβαση στα δεδομένα. Για παράδειγμα, η υπηρεσία πρόσβασης σε μια βάση δεδομένων που επιτρέπει στους χρήστες να προσπελάσουν τα δεδομένα που αυτή περιέχει.
- *Υλικά Στοιχεία (Physical assets):* Η κατηγορία αυτή περιλαμβάνει τα υλικά στοιχεία που αποτελούν το υπολογιστικό σύστημα, δηλαδή τους υπολογιστές, το δίκτυο, μέσα αποθήκευσης κτλ.
- *Τοποθεσίες (Locations):* Στην κατηγορία αυτή περιλαμβάνονται τα δωμάτια, κτίρια ή ακόμα και οικόπεδα τα οποία ανήκουν στον οργανισμό και περιέχουν μέρη των υπολογιστικών συστημάτων.
- *Στοιχεία Λογισμικού (Software assets):* Η κατηγορία αυτή περιλαμβάνει το λογισμικό που υποστηρίζει κάθε περιουσιακό στοιχείο δεδομένων.

Τα περιουσιακά στοιχεία συσχετίζονται άμεσα μεταξύ τους. Για παράδειγμα, τα δεδομένα μιας βάσης δεδομένων συσχετίζονται με την υπηρεσία πρόσβασης της βάσης δεδομένων, με τον υπολογιστή που περιέχει την βάση δεδομένων καθώς και με το δωμάτιο που βρίσκεται αυτός ο υπολογιστής. Το μοντέλο αυτό μπορεί να επεκταθεί ακόμα περισσότερο και να περιλάβει το δίκτυο που χρησιμοποιείται για την μεταφορά των δεδομένων, τους προσωπικούς υπολογιστές των χρηστών που έχουν πρόσβαση στα δεδομένα καθώς και ό,τι άλλο θέλουμε να περιλάβουμε.

Η λογική της δημιουργίας του μοντέλου είναι ότι το κάθε στοιχείο μεταφέρει ή προσθέτει απειλές και ευπάθειες στο άλλο. Για παράδειγμα, η εκδήλωση φωτιάς σε ένα δωμάτιο απειλεί τους υπολογιστές που περιέχονται σε αυτό, και επομένως και τις υπηρεσίες και δεδομένα που υπάρχουν στους υπολογιστές.

Τέλος, στην μέθοδο CRAMM τα περιουσιακά στοιχεία που αξιολογούνται είναι μόνο τα δεδομένα και τα υλικά στοιχεία. Θεωρείται ότι οι υπηρεσίες δεν έχουν αξία από μόνες τους, απλά περιέχουν την αξία των δεδομένων που προσφέρουν ή επεξεργάζονται. Η αξιολόγηση των υλικών στοιχείων είναι απλή, καθώς υπολογίζεται η τρέχουσα οικονομική τους αξία με βάση κλίμακα που προκαθορίζεται από τη μέθοδο.

Η αξιολόγηση των δεδομένων γίνεται με διαφορετικό τρόπο. Συγκεκριμένα, υπολογίζεται το αντίκτυπο που θα έχει στον οργανισμό η μη διαθεσιμότητα, μη εξουσιοδοτημένη αποκάλυψη, μετατροπή και καταστροφή των δεδομένων. Το αντίκτυπο που υπολογίζεται αντικατοπτρίζει πάντα την χειρότερη περίπτωση (worst case). Ο υπολογισμός του αντίκτυπου γίνεται με βάση κλίμακα από το 1 έως το 10 και με χρήση οδηγιών (guidelines) που περιέχει η μέθοδος. Οι

οδηγίες αυτές περιέχουν κατάλογο με τους πιθανούς τύπους αντίκτυπων, ώστε να καλύπτονται όλες οι περιπτώσεις, καθώς δεν είναι πάντοτε δυνατός ο υπολογισμός του οικονομικού αντίκτυπου. Για παράδειγμα η απώλεια δεδομένων μπορεί να επιφέρει οικονομικό αντίκτυπο, νομικό αντίκτυπο, ηθικό αντίκτυπο (λόγω απώλειας προσωπικών δεδομένων), ακόμα και την απειλή ανθρώπινης ζωής σε ορισμένες περιπτώσεις.

Α. Αναγνώριση Δεδομένων (Data assets)

Αξίζει να σημειωθεί ότι αφού ένα ΠΣΥ ενός δικτύου εξετάζει την ασφάλεια ιατρικών δεδομένων (εμπιστευτικές πληροφορίες), η εμπιστοσύνη και η αξιοπιστία είναι οι βασικές υπηρεσίες του συστήματος. Επομένως, ένα περιστατικό ασφάλειας δεν είναι μόνο ένα εσωτερικό πρόβλημα (κόστος αντικατάστασης), αλλά έχει άμεση επίδραση στην εμπιστοσύνη των ασθενών στο σύστημα και ως εκ τούτου στην ικανότητα του συστήματος να προσφέρει αξιόπιστες υπηρεσίες υγειονομικής περίθαλψης. Συνεπώς, η αποτίμηση των δεδομένων γίνεται σύμφωνα με την εκτίμηση της επίδρασης που θα μπορούσε να προκληθεί από την απώλεια της διαθεσιμότητας των δεδομένων ή/και την εμπιστευτικότητα των δεδομένων ή/και την ακεραιότητα των δεδομένων, λαμβάνοντας πάντα υπόψη το χειρότερο σενάριο. Τα περιουσιακά στοιχεία κατηγοριοποιούνται στις ακόλουθες κλάσεις: Ιατρικά Αρχεία Ασθενών, Κωδικοποιημένα Ιατρικά δεδομένα, Δεδομένα Αναφορών, Δεδομένα Ηχογραφήσεων.

Όμως, πρέπει να οριστεί ένας πιο ακριβής καθορισμός των κατηγοριών των δεδομένων που αποστέλλονται εντός ενός ΠΔΥ μέσω των συνιστωσών ενός ΠΠΣΥ, ακολουθούμενος από μια χαρτογράφηση μεταξύ των δεδομένων και των διαδικασιών. Οι βασικές κατηγορίες δεδομένων σε αυτά τα συστήματα είναι:

- Ιατρικά Δεδομένα
- Προσωπικά Δεδομένα
- Δεδομένα Διαχείρισης Ασθενών (Patient Management Data)
- Κλινικά Πρωτόκολλα
- Ευρετήρια Δεδομένων για την ολοκλήρωση διαδικασιών πχ. Κύριος κατάλογος δεδομένων των ασθενών για την ολοκλήρωση του Ηλεκτρονικού Αρχείου Υγείας
- Οικονομικά/ Εφοδιαστικά (Logistics) Δεδομένα
- Δεδομένα του Πληροφοριακού Συστήματος Διοίκησης (Management Information System)/ Δεδομένα Επιχειρησιακής Νοημοσύνης (Business Intelligence data)
- Διοικητικά Δεδομένα
- Δεδομένα Συστήματος (συμπεριλαμβανομένων των αντιγράφων ασφαλείας, δεδομένα σύμβασης του επιπέδου παροχής υπηρεσιών).

Ένα παράδειγμα για την χαρτογράφηση διαδικασιών και δεδομένων παρουσιάζεται στον Πίνακα 5.1. Αυτό είναι ένα απλουστευμένο παράδειγμα, δεδομένου ότι εξετάζει ομάδες διαδικασιών και όχι συγκεκριμένες διαδικασίες, αλλά η ιδέα είναι παρόμοια.

Πίνακας 5.1 *Διαδικασίες και δεδομένα*

PROCESSES	**DATA**
Admission/Discharge/ Transfer Processes	Medical Data
	Patient Management Data
	Indexing data for integrating processes
	Administrative data
Scheduling appointments for patient	Patient Management Data
	Administrative Data
	Indexing data for integrating processes (appointments in region)

Β. Αναγνώριση Υλικών Στοιχείων (Physical assets) και Υπηρεσιών (End User Services) που υποστηρίζουν

Τα υλικά στοιχεία που απαιτούνται για την επιτυχή λειτουργία ενός ΠΠΣΥ είναι:

1. Application Network Server (ANS): Αυτός είναι ο κύριος ξενιστής σταθμός δικτύου που αποθηκεύει τα ιατρικά αρχεία ασθενών και διευκολύνει την αποκωδικοποίηση και των έλεγχό τους μέσω εξειδικευμένου λογισμικού ελέγχου. Επιπλέον, υποστηρίζει την καταγραφή όλων των επικοινωνιών μεταξύ των γιατρών, νοσοκομείων ή ασθενών.
2. Εκτυπωτές: Πρόκειται για έγχρωμους εκτυπωτές inkjet για την εκτύπωση γραφημάτων και εκτυπωτές laser για την εκτύπωση αναφορών και γραμμάτων.
3. Μέσα για αντίγραφα ασφάλειας (Back up Media): Μαγνητικές ταινίες για back up των δεδομένων που είναι αποθηκευμένα στον ANS.
4. Γραμμή Διαδικτύου: Αυτή η γραμμή χρησιμοποιείται για εφαρμογές κίνησης και την IP τηλεφωνία.
5. Πρωτόκολλο Επικοινωνίας: Νοεί το TCP/IP πρωτόκολλο που χρησιμοποιείται για οποιονδήποτε τύπο επικοινωνίας.

6. Backup Server: εξυπηρετεί εξυπηρετητές και συστήματα από όλο το ΠΠΣΥ, καθώς και υπολογιστές που ανήκουν στο προσωπικό (πχ. Γιατροί) μετά από αίτησή τους.
7. DNS Server: Η διαθεσιμότητα του εξυπηρετητή αυτού είναι απαραίτητη για τη σωστή λειτουργία του δικτύου. Η μη διαθεσιμότητα της υπηρεσίας συνεπάγεται ουσιαστικά στην μη διαθεσιμότητα όλων των υπολογιστών του δικτύου μέσω της χρήσης διευθύνσεων DNS.
8. Database Server για Έξυπνες Κάρτες (Smartcards): Η ΒΔ περιέχει απόρρητες πληροφορίες για τις έξυπνες κάρτες για χρήση σε νησίδες του ΠΔΥ. Η λειτουργία της υπηρεσίας αυτής είναι πολύ σημαντική καθώς επηρεάζει την πρόσβαση στις νησίδες σε όλο το ΠΔΥ και σχετίζεται άμεσα με την ασφάλεια του εξοπλισμού που περιέχεται στις νησίδες (από κλοπή, καταστροφή κτλ).
9. Authentication Server: Τα συστήματα αυτά περιέχουν απόρρητα δεδομένα για την πρόσβαση των χρηστών στις υπηρεσίες του ΠΠΣΥ (user account information). Κάθε φορά που ένας χρήστης θέλει να χρησιμοποιήσει έναν υπολογιστή σε μια νησίδα, πρέπει να εισάγει τον όνομα και τον κωδικό του. Το ίδιο για την πρόσβαση από το σπίτι του μέσω τηλεφωνικού δικτύου, ή για να δει το ηλεκτρονικό του ταχυδρομείο κτλ. Είναι περιττό να αναφέρουμε την σημασία της υπηρεσίας αυτής για την εύρυθμη λειτουργία όλου του ΠΔΥ.

Γ. Αναγνώριση Στοιχείων Λογισμικού (Software Assets) και Υπηρεσιών (End User Services) που υποστηρίζουν

Τα περιουσιακά στοιχεία λογισμικού που απαιτούνται για την παροχή ΠΠΣΥ είναι τα εξής:

1. Λογισμικό Ιατρικών Αρχείων: Χρησιμοποιείται για την διατήρηση και την επεξεργασία των ΗΑΥ των ασθενών.
2. Λογισμικό για την υποστήριξη Τηλεπαρακολούθησης Ασθενών: Αποτελεί μια εφαρμογή που συλλέγει βιοσήματα ασθενών που βρίσκονται υπό διαρκή επιτήρηση και τα στέλνει σε άλλες τοποθεσίες, όπου υπάρχει ιατρικό προσωπικό που λαμβάνει τις αντίστοιχες πληροφορίες από ομότιμους σταθμούς εργασίας.
3. Λογισμικό Υποστήριξης Καταγραφών: Διευκολύνει την συντήρηση ενός αρχείου καταγραφής των επικοινωνιών που γίνονται μέσω δικτύου. Επίσης, υποστηρίζει την εγγραφή φωνητικής επικοινωνίας και την αρχειοθέτηση ηλεκτρονικών εγγράφων και μηνυμάτων ηλεκτρονικού ταχυδρομείου που μπορεί να ανταλλάσσονται.
4. Λογισμικό Υποστήριξης Τηλεδιασκέψεων: Υποστηρίζει την εφαρμογή τηλεδιασκέψεων και μπορεί να μοντελοποιηθεί ως ένα προφίλ κινήσεων VBR (Variable Bit Rate).
5. Λογισμικό Συναλλαγής Βάσεων Δεδομένων: Υποστηρίζει την ανάκτηση και την ασφάλεια ΗΑΥ.

Δ. Τοποθεσίες

Οι τοποθεσίες που περιλαμβάνονται στην ανάλυση είναι οι εξής:

1. Server Room: Στο δωμάτιο αυτό υπάρχουν όλοι οι εξυπηρετητές
2. Backup Media Room: Στο δωμάτιο αυτό φυλάσσονται όλα τα μέσα αντιγράφων ασφαλείας.
3. Κτήρια όπου στεγάζονται ΝΠΣ κτλ

Ο καθορισμός των τοποθεσιών απαιτείται μόνο αν λαμβάνονται υπόψη οι κίνδυνοι από φυσικές και περιβαλλοντικές καταστροφές. Αντιθέτως, όπως στην περίπτωση που εξετάζουμε, το βήμα αυτό δεν είναι αναγκαίο.

Η έκταση της ασφάλειας που απαιτείται ουσιαστικά εξαρτάται από την αξία των περιουσιακών στοιχειών που προστατεύονται. Η αξιολόγηση των περιουσιακών στοιχείων γίνεται με βάση οδηγίες που παρέχει η CRAMM.

Α'. Αποτίμηση δεδομένων

Ο στόχος της αποτίμησης των δεδομένων είναι να καθοριστεί η σημασία τους για τον οργανισμό. Η αξία των δεδομένων είναι ένα από τα βασικά στοιχεία για την εκτίμηση των απαιτήσεων ασφάλειας. Η αξιολόγηση των δεδομένων βασίζεται στις συνέπειες που υφίστανται όταν αυτά επηρεάζονται με διάφορους τρόπους, συμπεριλαμβανομένου της μη διαθεσιμότητας, της καταστροφής, της αποκάλυψης-κλοπής και της τροποποίησης των εν λόγω δεδομένων. Επιπλέον, η CRAMM παρέχει ένα σύνολο κατευθυντήριων γραμμών που επιτρέπει στα σενάρια χειρότερων περιπτώσεων (worst case scenarios) να μεταφραστούν σε τιμές κλίμακας από 1-10, όπου 1 είναι μια πολύ χαμηλή τιμή και 10 μια πολύ υψηλή. Οι τιμές κλίμακας χρησιμοποιούνται αργότερα από την CRAMM για τον υπολογισμό των κινδύνων για το υπό εξέταση σύστημα.

Τα αποτελέσματα φαίνονται παρακάτω.

Πίνακας 5.2 *Αξιολόγηση δεδομένων*

	Unavailability										**Dest**		**Disclosure**			**Modification**		
Name	15M	1H	3H	12H	1D	2D	1W	2W	1M	2M	DP	DT	I	CPS	O	SE	WE	DM
Medical Data	8	8	9	9	10	10	10	10	10	10	8	10	9		9			10
Personal Data			4	4	5	5	6	6	6	7	6	8	7		7			8
Patient Management Data					4	4	6	6	7	7	5	6	6		6			8
Clinical Protocols			7	7	8	8	9	9	9	9	7	9	7		8			9
Data Indexes for Integrating Processes	5	5	6	6	7	7	8	8	8	8	7	8	8		9			9

Financial / Logistics		3	3	4	4	4	5	6	7	8	6	8	5		6			7
MIS Data / BI Data		2	2	3	3	3	4	4	5	5	5	7	5		6			7
Administrative Data				3	3	3	5	5	7	7	5	8	5		6			7
Systems Data					4	4	5	5	6	6	6	8	5		6			6

Μνημονικό:

DP = Καταστροφή των δεδομένων μέχρι το τελευταίο backup

DT = Ολική καταστροφή συμπεριλαμβανομένων και των backup

I = Κλοπή των δεδομένων από εσωτερικούς (insiders)

O = Κλοπή των δεδομένων από εξωτερικούς (outsiders)

DM = Μετατροπή των δεδομένων με πρόθεση

Αναλυτικές πληροφορίες για την αξιολόγηση των δεδομένων υπάρχουν στο Παράρτημα Α.

Β'. Αποτίμηση Υλικών Στοιχείων

Ενώ η αξία των δεδομένων είναι ύψιστης σημασίας για την εκτίμηση κινδύνων, τα υλικά περιουσιακά στοιχεία έχουν επίσης αξία για τον οργανισμό. Η αξίες των υλικών περιουσιακών στοιχείων συμβάλλουν στον υπολογισμό των κινδύνων και την επακόλουθη επιλογή αντιμέτρων. Στην περίπτωσή μας, η αξία των υλικών περιουσιακών στοιχείων βαθμολογήθηκε με βάση την κλίμακα που περιλαμβάνεται στην CRAMM και η οποία έχει ως εξής:

- 1 έως 1.000 ευρώ
- 2 1.000 – 10.000
- 3 10.000 – 30.000
- 4 30.000 – 100.000
- 5 100.000 – 300.000 κτλ.

Η αξία των συστημάτων φαίνεται στον παρακάτω πίνακα:

Πίνακας 5.3 *Αξιολόγηση υλικών στοιχείων*

Σύστημα	**Βαθμός Κλίμακας**
Application Network Server (ANS)	3
Εκτυπωτές	2
Backup Media	2
Γραμμή Διαδικτύου	1

Πρωτόκολλο Επικοινωνίας	1
Backup Server	3
DNS Server	2
Database Server	2
Authentication Server	2

Γ'. Αποτίμηση Στοιχείων Λογισμικού

Τα λογισμικά εφαρμογών μπορεί επίσης να έχει αξία στον οργανισμό. Οι αξίες των στοιχείων λογισμικού συμβάλλουν και αυτές στον υπολογισμό κινδύνων καθώς και την επακόλουθη επιλογή αντιμέτρων. Στις περισσότερες περιπτώσεις, τα στοιχεία λογισμικού αρκεί να αξιολογηθούν με τον ίδιο τρόπο όπως τα υλικά στοιχεία, που όπως είδαμε αφορά την αντικατάσταση ή ανακατασκευή του κόστους. Στην περίπτωση αυτή το μόνο που χρειάζεται είναι να εισαχθεί μια οικονομική αξία για φυσική καταστροφή.

Περιστασιακά, τα λογισμικά εφαρμογών μπορεί να έχουν τις δικές τους εγγενείς απαιτήσεις για εμπιστευτικότητα και ακεραιότητα (πχ αν ο ίδιος ο πηγαίος κώδικας είναι εμπορικά εμπιστευτικός). Σε αυτές τις περιπτώσεις, τα στοιχεία λογισμικού θα πρέπει να εκτιμηθούν με τον ίδιο τρόπο όπως τα περιουσιακά στοιχεία δεδομένων. Συνεπώς, αυτού του είδους η αξιολόγηση μπορεί να χρησιμοποιηθεί σε οργανισμούς που παράγουν λογισμικό και επομένως είναι ύψιστης σημασίας η προστασία του κώδικα.

Η αξία των στοιχείων λογισμικού για την ΠΑΥ είναι αγοραστικής σημασίας και η αξία τους φαίνεται στον Πίνακα 5.4

Πίνακας 5.4 *Αξιολόγηση στοιχείων λογισμικού*

Λογισμικό	**Βαθμός Κλίμακας**
Λογισμικό Ιατρικών Αρχείων	2
Λογισμικό για την Υποστήριξη Τηλεπαρακολούθησης Ασθενών	2
Λογισμικό Υποστήριξης Καταγραφών	2
Λογισμικό Υποστήριξης Τηλεδιασκέψεων	1
Λογισμικό Συναλλαγής Βάσεων Δεδομένων	2

5.4.2 Αναγνώριση και Αποτίμηση Απειλών και Ευπαθειών

Στο στάδιο αυτό της μεθόδου CRAMM αναγνωρίζονται οι διάφορες απειλές που πιθανόν να υπάρχουν προς κάθε περιουσιακό στοιχείο του οργανισμού. Το πρόγραμμα CRAMM έχει μια μεγάλη λίστα από απειλές από τις οποίες καλούμαστε να επιλέξουμε. Συγκεκριμένα, εξετάζοντας τα περιουσιακά στοιχεία κάθε ένα ξεχωριστά αντιστοιχίζουμε όλες τις απειλές που ταιριάζουν και έχουν νόημα. Οι απειλές, όπως και τα περιουσιακά στοιχεία, χωρίζονται σε κατηγορίες:

- Απειλές προς υπηρεσίες
- Απειλές προς υλικά στοιχεία
- Απειλές προς τοποθεσίες
- Απειλές προς δεδομένα

Για παράδειγμα, η απειλή μιας φωτιάς απειλεί μια τοποθεσία ενώ η απειλή να καεί ένας υπολογιστής σχετίζεται με υλικά στοιχεία. Μπορούμε επίσης να κατηγοριοποιήσουμε τις απειλές με βάση το περιεχόμενο τους στις παρακάτω κατηγορίες:

Αφού τελειώσει το στάδιο της αντιστοίχησης των απειλών τότε πρέπει να γίνει η αξιολόγηση της πιθανότητας να συμβεί μια απειλή σε κάθε περιουσιακό στοιχείο, καθώς και η ευπάθεια του προς την απειλή αυτή. Κάθε απειλή μπορεί να βαθμολογηθεί με μια από τις παρακάτω τιμές:

- very low
- low
- medium
- high
- very high

Η ευπάθεια ενός περιουσιακού στοιχείου προς μια απειλή βαθμολογείται με μια από τις παρακάτω τιμές:

- low
- medium
- high

Η CRAMM διαθέτει δύο μεθόδους με τις οποίες μπορεί να γίνει η παραπάνω αξιολόγηση. Την ταχεία αξιολόγηση (rapid risk assessment) και την μέθοδο των ερωτηματολόγιων. Κάθε μια από αυτές μπορεί να χρησιμοποιηθεί ή ακόμα και συνδυασμός των δύο. Στην μέθοδο των ερωτηματολόγιων, η CRAMM παράγει ένα πλήθος ερωτημάτων για κάθε ζεύγος απειλής – περιουσιακού στοιχείου. Οι ερωτήσεις αυτές είναι τύπου πολλαπλών επιλογών, όπου η κάθε απάντηση βαθμολογείται με ορισμένο αριθμό πόντων. Με την απάντηση όλων των ερωτήσεων το πρόγραμμα προσθέτει τους βαθμούς που μαζεύτηκαν και υπολογίζει την απειλή και την ευπάθεια με μια από τις παραπάνω κλίμακες (low, high κτλ). Για να λειτουργήσει σωστά η

μέθοδος, τα ερωτηματολόγια πρέπει να απαντηθούν από άτομα που γνωρίζουν πολύ καλά το περιουσιακό στοιχείο που αναλύεται, και πάντα με την βοήθεια ενός αναλυτή κινδύνων.

Η μέθοδος της ταχείας αξιολόγησης είναι πιο απλή και προφανώς πιο γρήγορη. Στην μέθοδο αυτή επιχειρείται να βρεθεί άμεσα ο βαθμός της απειλής ή της ευπάθειας με βάση οδηγίες (guidelines) που παρέχονται από την μέθοδο. Συγκεκριμένα, η απειλή βαθμολογείται για το πόσο συχνά μπορεί να επιφέρει μη διαθεσιμότητα, κλοπή, καταστροφή και μεταβολή των δεδομένων. Η ευπάθεια βαθμολογείται για την πιθανότητα να επέλθει η χειρότερη περίπτωση όταν πραγματοποιηθεί μια απειλή (να σημειωθεί ότι η χειρότερη περίπτωση είχε υπολογιστεί κατά την αξιολόγηση των περιουσιακών στοιχείων). Η μέθοδος αυτή απαιτεί, περισσότερο από την προηγούμενη, έμπειρα άτομα που γνωρίζουν πολύ καλά τα προβλήματα που υπάρχουν και μπορούν να κάνουν άμεσους υπολογισμούς των κινδύνων.

Συνεπώς, το επόμενο βήμα είναι η αποτίμηση των απειλών που αντιμετωπίζει το σύστημα, καθώς και ο εντοπισμός των ευπαθειών που μπορεί να επιτρέψουν σε ορισμένες απειλές να συμβούν. Αυτές, με τη σειρά τους, θα μας παρέχουν τις σχετιζόμενες με την ασφάλεια ανάγκες των χρηστών. Η αποτίμηση των απειλών και των ευπαθειών σε συνδυασμό με την αποτίμηση των περιουσιακών στοιχείων του συστήματος, χρησιμοποιούνται για τον υπολογισμό του επίπεδου κινδύνου που διατρέχει το κάθε περιουσιακό στοιχείο του συστήματος. Παρακάτω ακολουθεί μια λίστα των απειλών που θέτουν σε κίνδυνο την κάθε ομάδα περιουσιακών στοιχείων του συστήματος χωριστά.

Α. Απειλές ενάντια των περιουσιακών στοιχείων δεδομένων:

- Μεταμφίεση ταυτότητας του χρήστη από εσωτερικά ή εξωτερικά μέλη (Masquerading of User Identity by Insiders/Outsiders).
- Διείσδυση Επικοινωνιών (Communications Infiltration)
- Υποκλοπή Επικοινωνιών (Communication Interception)
- Χειρισμός Επικοινωνιών (Communication Manipulation)
- Βλάβη Επικοινωνιών (Communication Failure)
- Αποποίηση Ευθυνών (Repudiation)
- Τυχαία λανθασμένη δρομολόγηση (Accidental misrouting)
- Κλοπή από εσωτερικά ή εξωτερικά μέλη (Theft by Insiders/Outsiders)
- Βλάβη Λογισμικού Συστήματος ή Δικτύου (System or Network Software Failure)
- Εισαγωγή επιβλαβούς ή διασπαστικού λογισμικού (Introduction of damaging or Disruptive Software)
- Ενσωμάτωση κακόβουλου κώδικα (Embedding of malicious code)
- Τεχνική βλάβη του ξενιστή (Technical Failure of Host)
- Τεχνική βλάβη των συσκευών αποθήκευσης (Technical Failure of Storage Device)

- Βλάβη λογισμικού εφαρμογών (Application Software Failure)
- Σφάλματα Εργασιών (Operations Error)
- Έλλειψη προσωπικού (Staff Shortage)
- Σφάλματα χρηστών (User Error)
- Μη εξουσιοδοτημένη χρήση εφαρμογών (Unauthorized use of an application)

Β. Απειλές ενάντια των υλικών περιουσιακών στοιχείων

- Κακή χρήση των πόρων του συστήματος (Misuse of systems resources)
- Κλοπή από εσωτερικά ή εξωτερικά μέλη (Theft by Insiders/Outsiders)
- Εκ προθέσεως φθορά (Willful Damage)
- Διακοπή ρεύματος (Power Failure)
- Σφάλματα Εργασιών (Operations Error)
- Σφάλματα συντήρησης υλικών στοιχείων (Hardware Maintenance Error)
- Τεχνική βλάβη του ξενιστή (Technical Failure of Host)
- Τεχνική βλάβη των συσκευών αποθήκευσης (Technical Failure of Storage Device)
- Τεχνική βλάβη των συσκευών εκτύπωσης (Technical Failure of Print Device)
- Τεχνική βλάβη των συνιστωσών διανομής δικτύου (Technical Failure of Network Distribution Components)
- Τεχνική βλάβη των υπηρεσιών δικτύου (Technical Failure of Network Services)
- Βλάβη Λογισμικού Συστήματος ή Δικτύου (System or Network Software Failure)

C. Απειλές ενάντια των περιουσιακών στοιχείων λογισμικού

- Μη εξουσιοδοτημένη χρήση εφαρμογών (Unauthorized use of an application)
- Εισαγωγή επιβλαβούς ή διασπαστικού λογισμικού (Introduction of damaging or Disruptive Software)
- Τεχνική βλάβη της διεπαφής δικτύου (Technical Failure of Network Interface)
- Τεχνική βλάβη των υπηρεσιών δικτύου (Technical Failure of Network Services)
- Σφάλματα Εργασιών (Operations Error)
- Βλάβη Λογισμικού Συστήματος ή Δικτύου (System or Network Software Failure)
- Βλάβη λογισμικού εφαρμογών (Application Software Failure)
- Σφάλματα συντήρησης λογισμικού (Software Maintenance Error)
- Κακή χρήση των πόρων του συστήματος (Misuse of systems resources)
- Ενσωμάτωση κακόβουλου κώδικα (Embedding of malicious code)
- Σφάλματα χρηστών (User Error)

D. Τοποθεσίες

- Πυρκαγιά
- Πλημμύρα
- Φυσικές καταστροφές
- Τρομοκρατία
- Διακοπή ρεύματος
- Διακοπή λειτουργίας του συστήματος κλιματισμού
- Κλοπή από εσωτερικά/εξωτερικά μέλη
- Εκ προθέσεως φθορά

Συνοψίζοντας τα παραπάνω, μπορούμε να καταλήξουμε στις απειλές που είναι πιθανόν να προσβάλλουν την εύρυθμη λειτουργία του ΠΠΣΥ ανά κατηγορία:

Α. Φυσικές καταστροφές

Οι απειλές που οφείλονται σε φυσικές καταστροφές μπορεί να διαφοροποιούνται από περιοχή σε περιοχή.

- Απειλή σεισμού (Α.1)
- Απειλή πλημμύρας (Α.2)

Β. Φυσικό και θεσμικό περιβάλλον

Μερικές από τις ακόλουθες απειλές ενδέχεται επίσης να διαφοροποιούνται από εγκατάσταση σε εγκατάσταση.

- Πιθανότητα εκδήλωσης πυρκαγιάς στο χώρο της εγκατάστασης (Β.1)
- Πιθανότητα εκδήλωσης πυρκαγιάς σε γειτονικές εγκαταστάσεις (Β.2)
- Πιθανότητα διαρροής υδάτων λόγω παλαιότητας ή κακής κατασκευής του δικτύου υδροδότησης (Β.3)
- Πιθανότητα αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση (Β.4)
- Πιθανότητα παραβίασης του νομικού πλαισίου που διέπει τις διαδικασίες μετάδοσης πληροφορίας και τήρησης αρχείων προσωπικών δεδομένων (Β.5)
- Πιθανότητα αδυναμίας υποστήριξης των ταχυτήτων του συστήματος από το παρεχόμενο από το κράτος δίκτυο μετάδοσης πληροφορίας (Β.6)

Γ. Ανθρώπινος παράγοντας

- Πιθανότητα αλλοίωσης, υποκλοπής ή καταστροφής μεταδιδόμενων πληροφοριών (Γ.1)
- Πιθανότητα πρόσβασης σε απόρρητες βάσεις δεδομένων και κοινοποίηση του περιεχομένου τους ή παραποίηση αυτού (Γ.2)
- Πιθανότητα προσβολής του συστήματος από την επιδρομή hacker (Γ.3)

- Πιθανότητα δολιοφθορών από δυσαρεστημένα στελέχη είτε των νοσοκομείων είτε της ανάδοχου εταιρείας (Γ.4)

Δ. Απειλές Τεχνολογίας

- Πιθανότητα χρησιμοποίησης νέων τεχνολογιών που θα αποδειχθούν μη λειτουργικές στο μέλλον (Δ.1)
- Πιθανότητα χρησιμοποίησης τεχνολογίας που θα καταστεί απαρχαιωμένη στο άμεσο μέλλον (Δ.2)
- Αδυναμία διασύνδεσης τμημάτων του έργου (Δ.3)
- Αδυναμία διασύνδεσης υπάρχοντος εξοπλισμού με το νέας τεχνολογίας εγκαθιστάμενο σύστημα (Δ.4)
- Πιθανότητα εγκατάστασης ελαττωματικού εξοπλισμού (Δ.5)

Ε. Επιχειρησιακές Απειλές

- Πιθανότητα αδυναμίας χρήσης του συστήματος λόγω έλλειψης ειδικών γνώσεων από το διοικητικό προσωπικό των νοσοκομείων (Ε.1)
- Πιθανότητα καταστροφής υλικού ή λογισμικού από τους χειριστές του συστήματος λόγω κακής χρήσης του (Ε.2)
- Πιθανότητα απροθυμίας προσαρμογής του προσωπικού των νοσοκομείων στα νέα δεδομένα του εργασιακού τους περιβάλλοντος (Ε.3)
- Ατελείς έλεγχοι από το προσωπικό ασφαλείας που δεν αντιλαμβάνεται την αξία της σωστής εκτέλεσης των καθηκόντων του (Ε.4)
- Πιθανότητα εσφαλμένης εγκατάστασης υλικού και λογισμικού από το προσωπικό της ανάδοχου εταιρείας, λόγω έλλειψης τεχνικών γνώσεων ή εξαιτίας απλού ανθρώπινου σφάλματος (Ε.5)

Αν μια από τις παραπάνω απειλές υλοποιηθεί και μετατραπεί σε περιστατικό σε σχέση με μια ομάδα περιουσιακών στοιχείων, μπορεί να επιφέρει ορισμένες επιπτώσεις – αντίκτυπα (για παράδειγμα μη διαθεσιμότητα για λιγότερο από 15 λεπτά, φυσική καταστροφή, σκόπιμη τροποποίηση). Για να υπολογιστούν ακριβώς τα μέτρα κινδύνων, η CRAMM πρέπει να ξέρει τις επιπτώσεις που θα μπορούσαν να προκύψουν σε συνάρτηση με κάθε πιθανό συνδυασμό απειλής/ομάδα περιουσιακών στοιχείων. Η μέθοδος CRAMM έχει προεπιλογές για τις επιπτώσεις που θα μπορούσαν να προκληθούν από κάθε απειλή. Περισσότερες πληροφορίες δίνονται σε Πίνακα του Παραρτήματος Β. Γενικά, το αντίκτυπο και οι επιπτώσεις των απειλών είναι καλά ορισμένα σε οδηγίες του Ινστιτούτου Διακυβέρνησης Πληροφορικής (Information Technology Governance Institute) και θα μπορούσαν να είναι:

- Άμεσες ή έμμεσες οικονομικές απώλειες

- Νομικές Συνέπειες
- Δυσφήμηση

Τα ακόλουθα πρέπει να προστεθούν συγκεκριμένα για το περιβάλλον ΠΔΥ:

- Έλλειψη διαλειτουργικότητας μεταξύ υφιστάμενων θέσεων ΤΠ και ΠΠΣΥ
- Μείωση της ποιότητας των παρεχόμενων υπηρεσιών προς τους ασθενείς και τους πολίτες.

Στη συνέχεια, για να υπολογιστεί το μέγεθος των απαιτήσεων ασφάλειας, είναι απαραίτητο να γίνει μια εκτίμηση τόσο για το επίπεδο απειλών ως προς τα περιουσιακά στοιχεία, όσο και για την έκταση των ευπαθειών των περιουσιακών στοιχείων ως προς αυτές τις απειλές. Οι απειλές που εντοπίστηκαν μπορούν να κατηγοριοποιηθούν σύμφωνα με την πιθανότητα εμφάνισής τους σε πέντε διαφορετικά επίπεδα. Για καλύτερη κατανόηση δίνεται παρακάτω μια ενδεικτική αποκωδικοποίηση της κλίμακας απειλών.

- Very low: ένα επεισόδιο δεν αναμένεται να συμβεί, κατά μέσο όρο, συχνότερα από μια φορά κάθε 10 χρόνια
- Low: ένα επεισόδιο αναμένεται να συμβεί, κατά μέσο όρο, κάθε 3 χρόνια
- Medium: ένα επεισόδιο αναμένεται να συμβεί, κατά μέσο όρο, κάθε χρόνο
- High: ένα επεισόδιο αναμένεται να συμβεί, κατά μέσο όρο, κάθε 4 μήνες
- Very high: ένα επεισόδιο αναμένεται να συμβεί, κατά μέσο όρο, κάθε μήνα.

Ο βαθμός της ευπάθειας είναι ενδεικτικός για το πόσο εύκολα μπορεί να συμβεί μεγάλη ζημιά σε περίπτωση που συμβεί κάποιο επεισόδιο. Συγκεκριμένα, μας λέει πόσο πιθανό είναι να συμβεί η χειρότερη περίπτωση. Η κλίμακα ευπαθειών κατηγοριοποιείται σε τρία διαφορετικά επίπεδα τα οποία είναι τα εξής:

- Low: εάν συνέβαινε ένα περιστατικό, δεν θα υπήρχε περισσότερο από 33% πιθανότητα να συμβεί το χειρότερο σενάριο (που αξιολογείται κατά την διάρκεια αποτίμησης περιουσιακών στοιχείων).
- Medium: εάν επρόκειτο να συμβεί ένα περιστατικό, η πιθανότητα να συμβεί το χειρότερο σενάριο κυμαίνεται από 33%-66% (που αξιολογείται κατά την διάρκεια αποτίμησης περιουσιακών στοιχείων).
- High: εάν ένα περιστατικό επρόκειτο να συμβεί, θα υπάρξει πιθανότητα υψηλότερη από 66% να συμβεί το χειρότερο σενάριο (που αξιολογείται κατά την διάρκεια αποτίμησης περιουσιακών στοιχείων).

Το ακόλουθο Σχήμα παρουσιάζει ένα δείγμα της συνοπτικής αναφοράς των απειλών και ευπαθειών. Περισσότερες πληροφορίες δίνονται στο Παράρτημα Β.

	Threat	Vulnerability
Masquerading of user identity by insiders-outsiders		
Medical Data	Medium	Medium
Personal Data	Medium	Medium
Patient Management Data	Medium	Medium
Clinical Protocols	Low	Medium
Data Indexes for Integrating Processes	Medium	Low
Financial/Logistics	Medium	High
MIS Data – BI Data	Low	Low
Administrative Data	Medium	High
Systems Data	Medium	Medium
Communication Infiltration		
Medical Data	Medium	Medium
Personal Data	High	Medium
Patient Management Data	Low	Low
Clinical Protocols	Low	Medium
Data Indexes for Integrating Processes	Medium	Medium
Financial/Logistics	Medium	High
MIS Data – BI Data	Low	Low
Administrative Data	Medium	High
Systems Data	Medium	Medium
Communication Interception		
Medical Data	Medium	Medium
Personal Data	Low	Low
Patient Management Data	Very Low	Medium
Clinical Protocols	Very Low	Medium
Data Indexes for Integrating Processes	Very Low	Low
Financial/Logistics	Medium	High
MIS Data – BI Data	Low	Low

Administrative Data	Very High	Medium
Systems Data	Medium	Medium
Communication Manipulation		
Medical Data	Low	Medium
Personal Data	Very Low	Low
Patient Management Data	Low	Low
Clinical Protocols	Very Low	Low
Data Indexes for Integrating Processes	Very Low	Low
Financial/Logistics	High	High
MIS Data – BI Data	Low	Low
Administrative Data	Very High	High
Systems Data	Low	Low

Σχήμα 5.4 *Αποτίμηση απειλών και ευπαθειών*

5.4.3 Υπολογισμός Κινδύνων

Ο υπολογισμός του βαθμού του κινδύνου με την μέθοδο CRAMM γίνεται με την χρήση ενός πίνακα «κινδύνου» ο οποίος παρέχεται. Η λογική πίσω από τον υπολογισμό είναι ο συνδυασμός των τιμών της αξίας, απειλής και ευπάθειας ώστε να παραχθεί ένα νούμερο που να είναι ενδεικτικό του «κόστους» που έχει στον οργανισμό η κάθε απειλή. Η κλίμακα του κίνδυνου στην CRAMM κυμαίνεται από το 1 (πολύ μικρός κίνδυνος) έως το 7 (πολύ μεγάλος κίνδυνος). Ο βαθμός αντικατοπτρίζει και το επίπεδο των απαιτήσεων ασφαλείας καθώς μεγάλος κίνδυνος υποδεικνύει υψηλές απαιτήσεις ασφαλείας. Παρακάτω φαίνεται ο πίνακας «κινδύνου» βάσει του οποίου γίνονται οι υπολογισμοί.

Πίνακας 5.5 *Πίνακας υπολογισμού κινδύνου*

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln. / Asset Value	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Η μεθοδολογία CRAMM υπολογίζει αυτόματα τον βαθμό του κινδύνου όταν ολοκληρωθούν τα προηγούμενα στάδια αξιολόγησης των περιουσιακών στοιχείων, απειλών και ευπαθειών. Κάποια αποτελέσματα από την ανάλυση στην ΠΑΥ φαίνονται στην επόμενη σελίδα. Αναλυτικά αποτελέσματα υπάρχουν στο Παράρτημα Β.

	Threat	**Vulnerability**	**MoR**
Masquerading of user identity by insiders-outsiders			
Medical Data	Medium	Medium	6
Personal Data	Medium	Medium	5
Patient Management Data	Medium	Medium	4
Clinical Protocols	Low	Medium	3
Data Indexes for Integrating Processes	Medium	Low	3
Financial/Logistics	Medium	High	5
MIS Data – BI Data	Low	Low	3
Administrative Data	Medium	High	5
Systems Data	Medium	Medium	3
Communications infiltration			
Medical Data	Medium	Medium	6
Personal Data	High	Medium	6

Patient Management Data	Low	Low	3
Clinical Protocols	Low	Medium	3
Data Indexes for Integrating Processes	Medium	Medium	4
Financial/Logistics	Medium	High	5
MIS Data – BI Data	Low	Low	3
Administrative Data	Medium	High	5
Systems Data	Medium	Medium	3
Communication Interception			
Medical Data	Medium	Medium	6
Personal Data	Low	Low	4
Patient Management Data	Very Low	Medium	3
Clinical Protocols	Very Low	Medium	3
Data Indexes for Integrating Processes	Very Low	Low	2
Financial/Logistics	Medium	High	5
MIS Data – BI Data	Low	Low	3
Administrative Data	Very High	Medium	5
Systems Data	Medium	Medium	3
Communication Manipulation			
Medical Data	Low	Medium	6
Personal Data	Very Low	Low	4
Patient Management Data	Low	Low	3
Clinical Protocols	Very Low	Low	2
Data Indexes for Integrating Processes	Very Low	Low	2
Financial/Logistics	High	High	5
MIS Data – BI Data	Low	Low	3
Administrative Data	Very High	High	6

Systems Data	Low	Low	2

Σχήμα 5.5 *Υπολογισμός βαθμού κινδύνου*

Όπως φαίνεται στον παραπάνω πίνακα, μερικές απειλές ξεχωρίζουν ως προς το κίνδυνο που δημιουργούν. Ιδιαίτερη προσοχή πρέπει να δοθεί σε αυτές που βαθμολογήθηκαν από 4-7, οπότε και πρέπει να δοθεί βαρύτητα για την αντιμετώπιση τους γιατί έχουν το μεγαλύτερο αντίκτυπο στο ΠΔΥ. Αυτό δεν σημαίνει, όμως, ότι οι υπόλοιπες απειλές δεν πρέπει να λαμβάνονται υπόψη. Αντιθέτως, όλες οι απειλές πρέπει να αντιμετωπίζονται η κάθε μια ανάλογα με την βαρύτητα της, διότι είναι γνωστό ότι η ασφάλεια ενός πληροφοριακού συστήματος είναι τόσο ισχυρή όσο ο πιο αδύναμος της κρίκος. Πρέπει να σημειωθεί ότι ο βαθμός του κινδύνου δείχνει ποια περιουσιακά στοιχεία είναι ποιο ευαίσθητα και πρέπει να προστατευτούν αλλά δεν υπολογίζει τα αντίμετρα που ενδεχομένως ήδη υπάρχουν εγκατεστημένα. Δηλαδή μπορεί κάτι να έχει υψηλό βαθμό κινδύνου αλλά να αντιμετωπίζεται ικανοποιητικά από τα υπάρχοντα μέτρα προστασίας.

5.5 Διαχείριση Κινδύνων – Αντίμετρα

Η διαχείριση κινδύνων έχει ως αντικείμενο την αντιμετώπιση τους και ουσιαστικά στοχεύει στο μετριασμό των ίδιων των κινδύνων και των επιπτώσεων τους. Περιλαμβάνει τον καθορισμό προτεραιοτήτων και την αξιολόγηση και εφαρμογή των κατάλληλων μέτρων αντιμετώπισης των κινδύνων που απειλούν το ΠΔΥ, είτε μειώνοντας τη πιθανότητα εμφάνισής τους είτε μετριάζοντας τις δυσμενείς επιπτώσεις από την εμφάνιση αυτών. Επειδή η πλήρης αποβολή των κινδύνων είναι συνήθως μη εφικτή, απώτερος σκοπός είναι να εφαρμοστούν τα μέτρα με το χαμηλότερο κόστος και τη μεγαλύτερη καταλληλότητα για να μειωθεί ο βαθμός έκθεσης του δικτύου σε κίνδυνο σε αποδεκτό επίπεδο, με τις μικρότερες δυνατές παραχωρήσεις όσον αφορά στην ποιότητά του και στην επίτευξη των στόχων για τους οποίους υλοποιείται.

Η CRAMM έχει μια τεράστια βάση δεδομένων από αντίμετρα κάθε τύπου που αντιμετωπίζουν όλες τις απειλές. Τα αντίμετρα αυτά όμως έχουν διαφορετική αποτελεσματικότητα και διαφορετικό κόστος υλοποίησης μεταξύ τους. Γι' αυτό το λόγο πρέπει να γίνει μια επιλογή των κατάλληλων αντιμέτρων για κάθε περίπτωση. Η CRAMM το πετυχαίνει αυτό λαμβάνοντας υπόψη τον τύπο του κάθε περιουσιακού στοιχείου, τις απειλές προς αυτό και τον βαθμό κινδύνου που έχει. Ο τύπος και οι απειλές καθορίζουν τον τύπο των αντιμέτρων ενώ ο βαθμός κινδύνου καθορίζει το κόστος υλοποίησης τους. Δηλαδή ένας υψηλός βαθμός κινδύνου δικαιολογεί και αντίμετρα με υψηλό κόστος υλοποίησης. Φυσικά ο υπολογισμός των αντιμέτρων από το εργαλείο CRAMM δεν είναι απλή υπόθεση και παίρνει αρκετό χρόνο ακόμα και με τους σύγχρονους υπολογιστές. Αυτό συμβαίνει επειδή τα αντίμετρα συνήθως δεν προστατεύουν από

μια μόνο απειλή αλλά από διάφορες απειλές. Και επίσης υπάρχουν αντίμετρα που προστατεύουν, αντίμετρα που ανιχνεύουν, αντίμετρα που μειώνουν το αντίκτυπο κτλ. Επίσης, τα αντίμετρα συνήθως αλληλεπικαλύπτουν το ένα το άλλο και τελικά η διαδικασία της επιλογής τους δεν είναι εύκολη.

Τα αντίμετρα που παράχθηκαν από την CRAMM για την ανάλυση κινδύνων που έγινε στο ΠΔΥ είναι πάρα πολλά και όλων των ειδών. Για την καλύτερη διαχείριση τους χωρίστηκαν στις παρακάτω κατηγορίες:

- Accounting (καταγραφή των κινήσεων σε log files κτλ)
- Audit (επίβλεψη ,εργαλεία για την ανάλυση των log files κτλ)
- Backup of data (αντίγραφα ασφαλείας των δεδομένων)
- Backup Tapes Controls (διαδικασίες για την προστασία των κασετών backup)
- Business Continuity Planning (διαδικασίες για την αντιμετώπιση περιστατικών)
- Compliance Checks (έλεγχοι για την επιβεβαίωση σωστής λειτουργίας αντιμέτρων κτλ.)
- Data Confidentiality over Networks (προστασία της εμπιστευτικότητας των δεδομένων που μεταδίδονται μέσω δικτύων δεδομένων)
- Environmental Protection (συνθήκες περιβάλλοντος στο δωμάτιο με τα πληροφοριακά συστήματα)
- Equipment Failure Protection (προστασία από βλάβες εξοπλισμού)
- Fire Protection (προστασία από φωτιά)
- Identification and Authentication (αναγνώριση και αυθεντικοποίηση χρηστών)
- Malicious Software (έλεγχοι και διαδικασίες για την αντιμετώπιση κακόβουλων προγραμμάτων)
- Power Protection (προστασία από προβλήματα ηλεκτροδότησης)
- Room Physical Security (προστασία φυσικής πρόσβασης στα δωμάτια)
- Software Change Controls (διαδικασίες αλλαγής λογισμικού)
- Software Maintenance Controls (διαδικασίες συντήρησης λογισμικού)
- System Administration Controls, (διαδικασίες διαχείρισης συστημάτων)
- Theft Protection (προστασία από κλοπές)
- Vulnerability Analysis (έλεγχοι για ευπάθειες και τρύπες ασφαλείας)
- Water Protection (προστασία από πλημμύρα).

Τα αντίμετρα που προτάθηκαν από το πρόγραμμα είναι μόνο ενδεικτικά. Δεν είναι απαραίτητη η υλοποίηση όλων των αντιμέτρων, μερικά δεν είναι καν εφαρμόσιμα στο συγκεκριμένο πληροφοριακό σύστημα. Η τελική επιλογή γίνεται πάντα από τους ανθρώπους που γνωρίζουν το σύστημα, τα προβλήματα του και δουλεύουν συνεχώς πάνω σε αυτό. Το πρόγραμμα δεν μπορεί σε καμία περίπτωση να αντικαταστήσει την γνώση αυτή. Παρ' όλα αυτά είναι επιθυμητό

να επιλεχθούν αντίμετρα από όλες τις κατηγορίες ώστε να υπάρχει μια πλήρης κάλυψη όλων των απειλών που υπάρχουν.

Λαμβάνοντας υπόψη τα αντίμετρα που παράχθηκαν από την CRAMM και τα προβλήματα που παρουσιάζονται κατά την ανάλυση κινδύνων, είμαστε σε θέση να συγκεκριμενοποιήσουμε τα αντίμετρα για κάθε απειλή που αναγνωρίστηκε σε προηγούμενη ενότητα (A1-E5), προτείνοντας δράσεις αντιμετώπισης για κάθε απειλή χωριστά.

Πίνακας 5.6 *Προτεινόμενες δράσεις αντιμετώπισης για κάθε απειλή*

Πιθανοί Κίνδυνοι	**Παρατηρήσεις και προτεινόμενη δράση αντιμετώπισης**
Α.1	Καμία δράση
Α.2	Τοποθέτηση συστημάτων σε όροφο, έλεγχος κουφωμάτων, ασφάλιση
Β.1	Σύστημα ανίχνευσης πυρκαγιάς, συστήματα πυρόσβεσης, τήρηση κανόνων ασφαλείας από το προσωπικό, ασφάλιση
Β.2	Η δράση για την αντιμετώπιση του Β.1 κινδύνου καλύπτει και τη δράση γι αυτόν το σχεδόν απίθανο κίνδυνο
Β.3	Έλεγχος του δωματίου όπου θα εγκατασταθεί το σύστημα (μικρής σημασίας έλεγχος)
Β.4	Έλεγχος των εγκαταστάσεων, ενημέρωση της αναθέτουσας αρχής για τις επιπλέον απαιτήσεις του έργου και εισαγωγή αυτών στον αρχικό σχεδιασμό υλοποίησης του έργου
Β.5	Μελέτη του νομικού πλαισίου που διέπει τη μετάδοση πληροφορίας και την τήρηση αρχείων προσωπικών δεδομένων και συμμόρφωση του σχεδιασμού υλοποίησης του έργου με αυτό (αναζήτηση της γνώμης ειδικών, πληροφόρηση για επικείμενες αλλαγές της νομοθεσίας)
Β.6	Πληροφόρηση για τις δυνατότητες του τρέχοντος δικτύου και για επικείμενη αναβάθμιση αυτού, υλοποίηση του έργου με βάση τις τρέχουσες δυνατότητες αυτού και παροχή της δυνατότητας εύκολης αναβάθμισης των συστημάτων
Γ.1	Κρυπτογράφηση μεταδιδόμενων πληροφοριών και γενικά εφαρμογή συνήθων μεθόδων ασφαλούς μετάδοσης πληροφορίας
Γ.2	Έλεγχος πρόσβασης με τεχνικά μέσα αλλά και με προσωπικό ασφαλείας (όχι υπερβολικά μέτρα)
Γ.3	Σύνηθες λογισμικό ασφάλειας δικτύων
Γ.4	Έλεγχος πρόσβασης σε υλικό, λογισμικό και βάσεις δεδομένων
Δ.1	Προσεκτική και τεκμηριωμένη επιλογή του επιπέδου τεχνολογίας που θα χρησιμοποιηθεί
Δ.2	Προσεκτική και τεκμηριωμένη επιλογή του επιπέδου τεχνολογίας που θα χρησιμοποιηθεί
Δ.3	Πλήρης αρχικός σχεδιασμός που θα προβλέπει τη δυνατότητα συνδεσιμότητας των τμημάτων του έργου
Δ.4	Ενημέρωση αναθέτουσας αρχής για τροποποιήσεις στον υπάρχον εξοπλισμό, εισαγωγή αυτών στον αρχικό σχεδιασμό υλοποίησης του έργου
Δ.5	Δυνατότητα άμεσης αντικατάστασης ελαττωματικού εξοπλισμού, πρόβλεψη τέτοιου είδους καθυστερήσεων στον αρχικό σχεδιασμό, τακτικός έλεγχος εξοπλισμού για πρόληψη καταστροφής και άλλων τμημάτων του έργου από τη χρήση μη ασφαλούς υλικού και

	λογισμικού
Ε.1	Εκπαίδευση του προσωπικού των νοσοκομείων που θα χειρίζεται το νέο σύστημα
Ε.2	Έλεγχος δυνατοτήτων προσωπικού, έλεγχος πρόσβασης προσωπικού σε ευπαθείς και υψηλού κόστους αποκατάστασης ζημιών τομείς του έργου
Ε.3	Θέσπιση κανόνων και ίσως ένα σεμινάριο παρουσίασης της αξίας του πληροφοριακού συστήματος
Ε.4	Θέσπιση κανόνων, έλεγχος άρτιας εκτέλεσης των καθηκόντων τους και ίσως ένα σεμινάριο παρουσίασης της αξίας του πληροφοριακού συστήματος
Ε.5	Έλεγχος γνώσεων του προσωπικού της αναδόχου εταιρείας (ενδεχομένως η ενέργεια αυτή να είναι περιττή καθώς κάθε εταιρία οφείλει πάντα να γνωρίζει τις ικανότητες του προσωπικού της)

5.6 Συμπεράσματα

Το κεφάλαιο αυτό επικεντρώνεται στην εκτίμηση κινδύνων ενός Ολοκληρωμένου Πληροφοριακού Συστήματος Υγείας (ΟΠΣΥ) στο πλαίσιο του ΠΔΥ. Συνήθως, η ανάλυση κινδύνων πραγματοποιείται για οργανισμούς υγείας, όπως νοσοκομεία ή κέντρα πρωτογενούς φροντίδας υγείας. Η τρέχουσα περίπτωση αποτελεί μια προσπάθεια να παρουσιαστεί η ανάλυση κινδύνων μεταξύ οργανισμών στον τομέα της υγειονομικής περίθαλψης. Ωστόσο, δεδομένου ότι δεν υλοποιούνται πολλά ΠΔΥ, η ανάλυση κινδύνων είναι αρκετά σύνθετη διαδικασία και παρουσιάζεται δυσκολία στην ολοκλήρωσή της.

Η μεθοδολογία ανάλυσης κινδύνων που παρουσιάζεται χρησιμοποιεί βασικά χαρακτηριστικά της CRAMM για την αναγνώριση των περιουσιακών στοιχείων, των απειλών και των ευπαθειών του ΟΠΣΥ, καθώς παρουσιάζεται και η μεταξύ τους σχέση σε ένα συνοπτικό και ευέλικτο πρότυπο. Μέσα από αυτήν την ανάλυση, εντοπίστηκαν οι μεγαλύτερες απειλές καθώς προτάθηκαν και πολλά αντίμετρα, προκειμένου να περιοριστούν οι ευπάθειες για την ομαλή λειτουργία του ΠΔΥ προς αυτές τις απειλές.

Λαμβάνοντας υπόψη την πολυπλοκότητα αυτών των συστημάτων, είναι προφανές ότι η ανάλυση κινδύνων είναι ένα διακριτό έργο που πρέπει να εφαρμόζεται παράλληλα σε όλες τις φάσεις σχεδιασμού και ανάπτυξης των συστημάτων ΠΔΥ.

Κεφάλαιο 6

Συμπεράσματα

Η ραγδαία εξέλιξη της τεχνολογίας συνδυασμένη με την ανάγκη για εύκολη πρόσβαση στην πληροφορία οδήγησε στη δημιουργία Πληροφοριακών Συστημάτων. Τα Πληροφοριακά Συστήματα βρίσκουν ολοένα και αυξανόμενες εφαρμογές στο χώρο της υγείας. Αποτελεί αδιαμφισβήτητο γεγονός ότι οι τεχνολογίες πληροφορικής και πληροφοριακών συστημάτων υγείας εφαρμόζονται και αξιοποιούνται. Παράλληλα, ανεξάρτητα από την πολυπλοκότητα των πληροφοριακών συστημάτων υγείας και των τεχνολογιών πληροφορικής, αυξάνονται ολοένα οι αποδέκτες τους και συνεχίζει η τεχνολογία αυτή να διαδίδεται.

Το διαδίκτυο, και οι εφαρμογές της τηλεϊατρικής αποτελούν μια εξαιρετικά ισχυρή καινοτομία που έχει επηρεάσει θα επηρεάζει και θα συνεχίσει να επηρεάζει και να διαμορφώνει τον τομέα της υγείας. Οι παραδοσιακές δομές και πρακτικές αλλάζουν και αναδιαμορφώνονται επηρεάζοντας τον τρόπο παράδοσης της ιατρικής φροντίδας προς τους ασθενείς, δημιουργώντας μια νέα τάξη πραγμάτων. Η παραδοσιακή σχέση γιατρού ασθενή περνάει σε μια άλλη διάσταση, αυτή του κυβερνοχώρου. Το επάγγελμα του ιατρού αποκτάει πλέον άλλη υπόσταση, προστίθενται σ' αυτό νέες ικανότητες και δεξιότητες. Οι σχεδιαστές πληροφοριακών συστημάτων υγείας πρέπει να λαμβάνουν υπόψη τους κατά τον σχεδιασμό ότι οι νέες τεχνολογίες είναι εδώ για να διευκολύνουν και να υπηρετήσουν τον άνθρωπο και όχι να στήνουν εμπόδια μπροστά του.

Ο χώρος της υγείας, είναι εξαιρετικά πολύπλοκος και είναι ιδιαίτερα δύσκολο στο να δοθούν σαφείς ορισμοί σχετικά με τα πληροφοριακά συστήματα που σχεδιάζονται για αυτόν. Στην διεθνή βιβλιογραφία, επικρατεί μία σύγχυση καθώς η ακριβής σημασία των όρων που χρησιμοποιούνται διαφοροποιείται ανάλογα με τον συγγραφέα, ερευνητή ή μελετητή. Στην εργασία αυτή επισημάνθηκαν μερικοί από τους επικρατέστερους ορισμούς. Παράλληλα, έγινε μια προσπάθεια να δομηθούν με τρόπο τέτοιο ώστε να γίνει κατανοητό το πλαίσιο μέσα στο οποίο λειτουργούν.

Τα οφέλη της εισαγωγής των τεχνολογιών πληροφορικής και επικοινωνιών στον ήδη σύνθετο χώρο της Υγείας και Πρόνοιας έχουν από καιρό αναγνωριστεί και επισημανθεί από τη Διεθνή βιβλιογραφία. Παρόλα αυτά, αναπτύσσονται θέματα και περιπτώσεις που αφορούν τη διασύνδεση των συστημάτων. Η παροχή υπηρεσιών υγείας από όλους όσους συμμετέχουν στα ΠΣΥ ή στα ΠΔΥ προϋποθέτει τη διακίνηση της πληροφορίας όπως αυτή αποκτάται και αποθηκεύεται πρωτογενώς. Συχνά η πληροφορία, ιδιαίτερα όταν αυτή αφορά τον ασθενή πρέπει να διακινηθεί άμεσα και να έχει τους σωστούς αποδέκτες όπως για παράδειγμα στην περίπτωση

διακομιδής του ασθενούς. Σε όλες τις περιπτώσεις δεν θα πρέπει να υπάρχουν σημασιολογικές απώλειες σε πληροφοριακό επίπεδο. Η ανάγκη για διακίνηση της πληροφορίας διευκολύνεται και από τις νέες τάσεις για εφαρμογή των εργαλείων και υπηρεσιών eHealth που οδηγούν στο κοινόχρηστο Ηλεκτρονικό Αρχείο Υγείας του ασθενή με σκοπό τη συνεχή φροντίδα της υγείας του, τη διακίνηση ηλεκτρονικών παραπεμπτικών κτλ.

Τα προβλήματα που πρέπει να αντιμετωπιστούν για την επίτευξη της κοινής χρήσης και της διακίνησης της πληροφορίας στο ΠΣΥ είναι:

- Το χαμηλό ποσοστό διαθεσιμότητας των ΠΣ στις διασυνδεδεμένες μονάδες υγείας, με αποτέλεσμα την δυσκολία στην ανταλλαγή δεδομένων
- Τα ετερογενή συστήματα, που στηρίζουν τις μονάδες υγείας σε συνδυασμό με την έλλειψη προτυποποίησης των επικοινωνιακών υποδομών
- Η ανάγκη αναδιοργάνωσης δομών και διαδικασιών, ώστε σε συνδυασμό με τις τεχνολογικές εξελίξεις να μπορούν να υποστηρίξουν την ανταλλαγή δεδομένων.

Γενικότερα, όταν τα ηλεκτρονικά δεδομένα μπορούν να οργανωθούν σε δομές και δομημένα μηνύματα ακολουθώντας δομημένη είσοδο δεδομένων και δομημένες κλινικές περιγραφές, η επικοινωνία γίνεται με πιο ασφαλή και ποιοτικό τρόπο χρησιμοποιώντας δομημένα μηνύματα και πληροφορία που ακολουθεί συγκεκριμένα πρότυπα όσον αφορά την καταγραφή της και την σημασιολογία της. Συνεπώς, είναι επιτακτική η θέσπιση κωδικών και προτύπων, τα οποία καθορίζουν τον τρόπο συλλογής, συνεργασίας και παρουσίασης των δεδομένων από διαφορετικά ΠΣ. Απαραίτητη λοιπόν θεωρείται η ύπαρξη ενός δικτύου, το οποίο με τη χρήση υλικού και πολλών ίσως επιπέδων και λειτουργικών μονάδων λογισμικού, θα καταφέρει να συνδέσει όλα τα ετερογενή συστήματα.

Τα ΠΣΥ και η Ηλεκτρονική Υγεία κουβαλούν μαζί τους ένα τεράστιο σύνολο απαιτήσεων. Η κυβέρνηση καλείται να υποστηρίξει τις απαιτήσεις αυτές θεσπίζοντας την κατάλληλη νομοθεσία, αναλαμβάνοντας έτσι τις ευθύνες της και εναρμονίζοντας την παρούσα νομοθεσία με την αναδυόμενη τεχνολογία καλύπτοντας τα διάφορα κενά που υπάρχουν. Η σύσταση και η λειτουργία των ΠΣΥ πρέπει να τηρεί τις αρχές προστασίας των δεδομένων προσωπικού χαρακτήρα όπως αυτές δίνονται από την οδηγία την Ευρωπαϊκής Ένωσης 95/46/ΕΚ. Μελετώντας αυτή την οδηγία, διαπιστώθηκε ότι η ερμηνεία της οδηγίας στο χώρο της υγείας ποικίλει και πολλές φορές οι απαγορευτικές αρχές που διατυπώνει μπορεί να επηρεάσουν τις λειτουργίες ενός οργανισμού. Επομένως, απαιτείται η επανεξέταση των θεμάτων ασφαλείας των πληροφοριών και επεξεργασίας τους εξειδικεύοντας την υφιστάμενη νομοθεσία στο χώρο της υγείας.

Μέχρι σήμερα στην υπάρχουσα νομοθεσία δεν υπάρχει κανόνας δεοντολογίας σχετικά με την ηλεκτρονική υγεία αλλά ούτε σαφείς αρχές που καθορίζουν την απόδοση ευθυνών σε

περιπτώσεις τεχνικών προβλημάτων των πληροφοριακών συστημάτων που σχετίζονται με την παροχή υγείας. Συνεπώς η προσαρμογή της νοσοκομειακής οργάνωσης στην τεχνολογική αλλαγή απαιτεί αλλαγές στο υπάρχον κανονιστικό πλαίσιο, αφού η σύγκλιση των τεχνολογιών, δεν συνεπάγεται αυτονόητα και την σύγκλιση των νομοθεσιών. Τίθενται μεγάλα ερωτήματα αλλά και προκλήσεις για τη διατήρηση της ασφάλειας και της προστασίας των δεδομένων αλλά και της διασφάλισης ότι μόνο εξουσιοδοτημένα άτομα θα έχουν πρόσβαση σε αυτά τα δεδομένα για νόμιμους πάντα σκοπούς.

Η έλλειψη βασικών νομοθεσιών που έπρεπε να ισχύουν πριν τη λειτουργία ΠΣΥ, επέφεραν καταστροφικά πλήγματα στα πρώτα στάδια υλοποίησης και εφαρμογής τέτοιων συστημάτων ανά το παγκόσμιο. Μέσα από τη μελέτη της νομοθεσίας που υπάρχει σε Ευρωπαϊκό και κατ' επέκταση σε παγκόσμιο επίπεδο, γίνεται σαφής ότι η νομοθεσία βρίσκεται σε ένα πρώιμο επίπεδο. Σε γενικές γραμμές η νομοθεσία δεν αποτρέπει την υλοποίηση και χρήση ηλεκτρονικών φακέλων ασθενών για σκοπούς πρωτοβάθμιας παροχής υπηρεσιών ή και για δευτεροβάθμιους σκοπούς, όπως είναι η έρευνα. Το παρόν νομοθετικό πλαίσιο δεν είναι πλήρως ανεπτυγμένο και απαιτεί καθοδήγηση και πολιτική θέληση έτσι ώστε να προωθήσει την ολοκλήρωση και την ευρεία χρήση των πληροφοριών των ΗΑΥ.

Στις μέρες μας, πολλές τεχνολογίες υιοθετούνται από τον ιατρικό τομέα. Οι τεχνολογίες αυτές παράγουν πολλά οφέλη για την παροχή υπηρεσιών υγείας, όμως, υπάρχουν διάφορες επιπτώσεις ενάντια τις ασφάλειας και της ιδιωτικότητας που πρέπει να διερευνηθούν προκειμένου να προωθηθούν και να διατηρηθούν οι θεμελιώδεις ιατρικές και ηθικές αρχές και κοινωνικές προσδοκίες. Τα ζητήματα αυτά περιλαμβάνουν τα δικαιώματα πρόσβασης σε δεδομένα, πώς και πότε αποθηκεύονται τα δεδομένα αυτά, την ασφάλεια μεταφοράς δεδομένων, τα δικαιώματα ανάλυσης δεδομένων και πολιτικές ασφάλειας. Στην εργασία αυτή, αναφέρθηκαν μερικές από τις υπάρχουσες λύσεις που μπορούν να υιοθετηθούν και οι απειλές που τις διέπουν και που πρέπει να λυθούν, ώστε να είναι δυνατή η ευρεία χρήση των νέων τεχνολογιών αυτών με τους ελάχιστους κινδύνους ενάντια της ασφάλειας και της ιδιωτικότητας.

Σε όλα όσα προηγήθηκαν έγινε σαφής η αξία και η επιτακτικότητα της εφαρμογής των διαδικασιών ανάλυσης κινδύνων σε ένα ΟΠΣΥ. Η ανάλυση κινδύνων, στην περίπτωσή μας χρησιμοποιώντας την μεθοδολογία CRAMM, είναι μια αυστηρά δομημένη διαδικασία της οποίας τα βήματα θα πρέπει να εκτελούνται με επιμέλεια και σύνεση, καθώς μόνο έτσι θα καταφέρει να επιτύχει τους στόχους της. Και ουσιαστικά στόχος της διαδικασίας ανάλυσης και διαχείρισης κινδύνων είναι η άρτια λειτουργία του ΠΣΥ, χωρίς να επηρεαστεί αυτή από απρόοπτα γεγονότα. Όλα τα στάδια της διαδικασίας ανάλυσης κινδύνων είναι εξίσου σημαντικά και έχουν τη δική τους ξεχωριστή συμβολή για την επίτευξη των στόχων της διαδικασίας.

Η αναγνώριση και αποτίμηση περιουσιακών στοιχείων θα αποτελέσει την πολύτιμη βάση δεδομένων που θα χρησιμοποιηθεί για την άντληση των απαιτούμενων πληροφοριών που απαιτούνται στα επόμενα στάδια. Η αναγνώριση και αποτίμηση των πιθανών απειλών πρέπει να πραγματοποιείται με ιδιαίτερη προσοχή καθώς θα πρέπει να συμπεριληφθούν όλοι οι κίνδυνοι που μπορούν να απειλήσουν το ΠΠΣΥ. Η αξιολόγηση των κινδύνων αποτελεί ίσως το πιο δύσκολο στάδιο της διαδικασίας καθώς εδώ θα πρέπει να εκτιμηθούν η πιθανότητα εμφάνισης της κάθε απειλής καθώς και οι επιπτώσεις τους και οι ευπάθειες των περιουσιακών στοιχείων, ώστε να εξαχθούν χρήσιμα συμπεράσματα για περαιτέρω δράση. Στη συνέχεια, προτείνονται τα μέτρα που πρέπει να τεθούν σε εφαρμογή για την προστασία του ΠΠΣΥ και των οποίων η αξία δε θα πρέπει να ξεπερνά το ενδεχόμενο κόστος των απωλειών από τους κινδύνους. Επίσης καταδεικνύεται και ο υπολειπόμενος κίνδυνος που δεν μπορεί να εξαλειφθεί πλήρως από τα μέτρα που ελήφθησαν.

Καθώς λοιπόν οι κίνδυνοι είναι ένα φαινόμενο το οποίο ο άνθρωπος καλούταν πάντα να αντιμετωπίσει και θα συνεχίσει να το αντιμετωπίζει και στο μέλλον, η χρήση τέτοιων ορθολογικών και επιστημονικών διαδικασιών όπως η ανάλυση κινδύνων θα είναι πάντοτε ένα χρήσιμο εργαλείο. Πολύ περισσότερο στην υλοποίηση ΟΠΣΥ εξαιτίας της πολυπλοκότητας αυτών αλλά και των νέων τεχνολογιών που αυτά εισάγουν.

Τέλος αξίζει να αναφέρουμε πως η επιτυχημένη κατάρτιση ενός σχεδίου ανάλυσης και διαχείρισης κινδύνων οφείλεται σε μεγάλο βαθμό στην εμπειρία, τις ικανότητες, την οξυδέρκεια, τη διορατικότητα και την επιμέλεια των προσώπων που θα κληθούν να το συντάξουν.

Παράρτημα Α

Στο παράρτημα αυτό υπάρχει η αναλυτική αξιολόγηση των δεδομένων της ΠΑΥ. Η αξιολόγηση γίνεται με βάση το αντίκτυπο που έχει η μη διαθεσιμότητα, καταστροφή, μη εξουσιοδοτημένη αποκάλυψη και μεταβολή με πρόθεση των δεδομένων.

Στους παρακάτω πίνακες, για κάθε τύπο δεδομένων υπάρχει λίστα με τους πιθανούς τύπους προβλημάτων (μη διαθεσιμότητα κτλ). Στην ίδια σειρά, στις 2 στήλες που υπάρχουν στα δεξιά φαίνεται ο τύπος του αντίκτυπου και ο βαθμός που του δόθηκε από την αξιολόγηση. Ορισμένα προβλήματα μπορεί να έχουν διάφορους τύπους αντίκτυπων ταυτόχρονα. Σε αυτές τις περιπτώσεις επιλέγεται το αντίκτυπο με τον μεγαλύτερο βαθμό. Παρακάτω εξηγούνται μερικές από τις κατηγορίες των αντίκτυπων για καλύτερη κατανόηση.

- Policy and Operations of Public Service: Αδυναμία σωστής λειτουργίας και εξυπηρέτησης των «πελατών».
- Financial Loss: Άμεσες οικονομικές απώλειες (πχ. Από κλοπή εξοπλισμού ή από απώλεια ανθρωποωρών)
- Loss of Goodwill: Σε αυτήν την κατηγορία αντίκτυπου ανήκουν όλες οι περιπτώσεις που μπορεί να φέρουν την ΠΑΥ σε δύσκολη θέση ως προς τα «έξω» (embarrassment) και να χαλάσουν το καλό όνομα του οργανισμού.
- Personal Information: Προβλήματα που προκύπτουν από την διαχείριση και αποθήκευση προσωπικών δεδομένων (πχ. Κλοπή). Συμπεριλαμβάνονται και νομικά προβλήματα.
- Management and business operations: Αδυναμία σωστής διαχείρισης και λειτουργίας του οργανισμού.
- Disruption to Activities: Έμμεσες οικονομικές απώλειες.
- Personal Safety: Σε αυτή την κατηγορία αντίκτυπου ανήκουν οι περιπτώσεις που μπορούν να προκαλέσουν μικρό τραυματισμό μέχρι και την απώλεια ανθρώπινης ζωής.

Data Asset Valuation

Data Asset	Medical Data
Type of Data	Sensitive
Interviewees	Konstantinos Lamprinoudakis
Interviewers	Evaggelia Karastamati
Date	26 Aug 2012
Status	Completed

Description of Data

Impacts

Unavailability – less than 15 minutes	Guideline	Scale Value	Financial Value
	Personal Safety	8	
Unavailability – 1 hour	Guideline	Scale Value	Financial Value
	Personal Safety	8	
Unavailability – 3 hours	Guideline	Scale Value	Financial Value

	Personal Safety	9	
Unavailability – 1 day	Guideline	Scale Value	Financial Value
	Personal Safety	10	
Unavailability – 2 weeks	Guideline	Scale Value	Financial Value
	Personal Safety	10	
Unavailability – 2 months	Guideline	Scale Value	Financial Value
	Personal Safety	10	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Personal Safety	8	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Personal Safety	10	
Unauthorized disclosure to insiders	Guideline	Scale Value	Financial Value
	Personal Safety	9	
Unauthorized disclosure to outsiders	Guideline	Scale Value	Financial Value
	Personal Safety	9	

Data Asset Valuation

Data Asset Personal Data

Type of Data	Personal
Interviewees	Konstantinos Lamprinoudakis
Interviewers	Evaggelia Karastamati
Date	26 Aug 2012
Status	Completed

Description of Data

Impacts

Unavailability – less than 15 minutes	Guideline	Scale Value	Financial Value
	Personal Information	3	
Unavailability – 1 hour	Guideline	Scale Value	Financial Value
	Personal Information	3	
Unavailability – 3 hours	Guideline	Scale Value	Financial Value
	Personal Information	4	
Unavailability – 1 day	Guideline	Scale Value	Financial Value
	Personal Information	5	
Unavailability – 2 weeks	Guideline	Scale Value	Financial Value
	Personal Information	6	
Unavailability – 2 months	Guideline	Scale Value	Financial Value
	Personal Information	7	
Destruction since the last successful	Guideline	Scale	Financial

back-up		Value	Value
	Personal Information	6	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Personal Information	8	
Unauthorized disclosure to insiders	Guideline	Scale Value	Financial Value
	Personal Information	7	
Unauthorized disclosure to outsiders	Guideline	Scale Value	Financial Value
	Personal Information	7	

Data Asset Valuation

Data Asset	Patient Management Data
Type of Data	Confidential
Interviewees	Konstantinos Lamprinoudakis
Interviewers	Evaggelia Karastamati
Date	26 Aug 2012
Status	Completed

Description of Data

Impacts			
Unavailability – less than 15 minutes	Guideline	Scale Value	Financial Value
	Management & Business Operations	1	
Unavailability – 1 hour	Guideline	Scale Value	Financial Value
	Management & Business Operations	1	
Unavailability – 3 hours	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 1 day	Guideline	Scale Value	Financial Value
	Management & Business Operations	4	
Unavailability – 2 weeks	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	
Unavailability – 2 months	Guideline	Scale Value	Financial Value
	Management & Business Operations	7	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Management & Business Operations	8	
Unauthorized disclosure to insiders	Guideline	Scale	Financial

		Value	Value
	Management & Business Operations	6	
Unauthorized disclosure to outsiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	

Asset Valuation

CRAMM **Confidential** **Review: ΠΑΥ**

Data Asset Valuation

Data Asset	Clinical Protocols
Type of Data	Confidential
Interviewees	Konstantinos Lamprinoudakis
Interviewers	Evaggelia Karastamati
Date	26 Aug 2012
Status	Completed

Description of Data

Impacts

Unavailability – less than 15 minutes	Guideline	Scale Value	Financial Value

	Personal Safety	6	
Unavailability – 1 hour	Guideline	Scale Value	Financial Value
	Personal Safety	6	
Unavailability – 3 hours	Guideline	Scale Value	Financial Value
	Personal Safety	7	
Unavailability – 1 day	Guideline	Scale Value	Financial Value
	Personal Safety	8	
Unavailability – 2 weeks	Guideline	Scale Value	Financial Value
	Personal Safety	9	
Unavailability – 2 months	Guideline	Scale Value	Financial Value
	Personal Safety	9	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Management & Business Operations	7	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Management & Business Operations	9	
Unauthorized disclosure to insiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	7	
Unauthorized disclosure to outsiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	9	

Data Asset Valuation

Data Asset	Data Indexes for Integrating Processes
Type of Data	Confidential
Interviewees	Konstantinos Lamprinoudakis
Interviewers	Evaggelia Karastamati
Date	26 Aug 2012
Status	Completed

Description of Data

Impacts

Unavailability – less than 15 minutes	Guideline	Scale Value	Financial Value
	Management & Business Operations	5	
Unavailability – 1 hour	Guideline	Scale Value	Financial Value
	Management & Business Operations	5	
Unavailability – 3 hours	Guideline	Scale Value	Financial Value
	Management & Business	6	

	Operations		
Unavailability – 1 day	Guideline	Scale Value	Financial Value
	Management & Business Operations	7	
Unavailability – 2 weeks	Guideline	Scale Value	Financial Value
	Management & Business Operations	8	
Unavailability – 2 months	Guideline	Scale Value	Financial Value
	Management & Business Operations	8	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Management & Business Operations	7	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Management & Business Operations	8	
Unauthorized disclosure to insiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	7	
Unauthorized disclosure to outsiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	9	

Data Asset Valuation

Data Asset	Financial - Logistics
Type of Data	Confidential
Interviewees	Konstantinos Lamprinoudakis
Interviewers	Evaggelia Karastamati
Date	26 Aug 2012
Status	Completed

Description of Data

Impacts

Unavailability – less than 15 minutes	Guideline	Scale Value	Financial Value
	Management & Business Operations	1	
Unavailability – 1 hour	Guideline	Scale Value	Financial Value
	Management & Business Operations	1	
Unavailability – 3 hours	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 1 day	Guideline	Scale Value	Financial Value
	Management & Business Operations	4	
Unavailability – 2 weeks	Guideline	Scale	Financial

		Value	Value
	Management & Business Operations	6	
Unavailability – 2 months	Guideline	Scale Value	Financial Value
	Management & Business Operations	8	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Management & Business Operations	8	
Unauthorized disclosure to insiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	5	
Unauthorized disclosure to outsiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	

Data Asset Valuation

Data Asset	MIS – Business Intelligence Data
Type of Data	Confidential

Interviewees	Konstantinos Lamprinoudakis
Interviewers	Evaggelia Karastamati
Date	26 Aug 2012
Status	Completed

Description of Data

Impacts

Unavailability – less than 15 minutes	Guideline	Scale Value	Financial Value
	Management & Business Operations	2	
Unavailability – 1 hour	Guideline	Scale Value	Financial Value
	Management & Business Operations	2	
Unavailability – 3 hours	Guideline	Scale Value	Financial Value
	Management & Business Operations	2	
Unavailability – 1 day	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 2 weeks	Guideline	Scale Value	Financial Value
	Management & Business Operations	4	
Unavailability – 2 months	Guideline	Scale Value	Financial Value

	Management & Business Operations	5	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Management & Business Operations	5	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Management & Business Operations	7	
Unauthorized disclosure to insiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	5	
Unauthorized disclosure to outsiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	

Data Asset Valuation

Data Asset	Administrative Data
Type of Data	Confidential
Interviewees	Konstantinos Lamprinoudakis
Interviewers	Evaggelia Karastamati
Date	26 Aug 2012
Status	Completed

Description of Data

Impacts

Unavailability – less than 15 minutes	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 1 hour	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 3 hours	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 1 day	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 2 weeks	Guideline	Scale Value	Financial Value
	Management & Business Operations	5	
Unavailability – 2 months	Guideline	Scale Value	Financial Value
	Management & Business Operations	7	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Management & Business Operations	5	

Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Management & Business Operations	8	
Unauthorized disclosure to insiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	5	
Unauthorized disclosure to outsiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	

Data Asset Valuation

Data Asset	Systems Data
Type of Data	Confidential
Interviewees	Konstantinos Lamprinoudakis
Interviewers	Evaggelia Karastamati
Date	26 Aug 2012
Status	Completed

Description of Data

Impacts

Unavailability – less than 15 minutes	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 1 hour	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 3 hours	Guideline	Scale Value	Financial Value
	Management & Business Operations	3	
Unavailability – 1 day	Guideline	Scale Value	Financial Value
	Management & Business Operations	4	
Unavailability – 2 weeks	Guideline	Scale Value	Financial Value
	Management & Business Operations	5	
Unavailability – 2 months	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Management & Business Operations	8	
Unauthorized disclosure to insiders	Guideline	Scale Value	Financial Value

	Management & Business Operations	5	
Unauthorized disclosure to outsiders	Guideline	Scale Value	Financial Value
	Management & Business Operations	6	

Παράρτημα Β

Στο παράρτημα αυτό, αρχικά, υπάρχει ο αναλυτικός Πίνακας Απειλών και Αντίκτυπων που παρέχεται από την CRAMM. Στη συνέχεια, παρουσιάζεται μια σύνοψη Πινάκων για την αποτίμηση απειλών και ευπαθειών, καταλήγοντας στους Πίνακες όπου παρουσιάζονται αναλυτικά τα αποτελέσματα του βαθμού κινδύνου που διατρέχουν τα περιουσιακά στοιχεία του ΠΔΥ.

Στους Πίνακες Υπολογισμού Κινδύνου, στην αριστερή στήλη αναγράφεται το όνομα της κάθε απειλής. Κάτω από την απειλή, στην ίδια στήλη, αναγράφεται το κάθε περιουσιακό στοιχείο που διατρέχει την απειλή αυτή. Δεξιά από την στήλη αυτή, ακολουθούν τρεις ακόμα στήλες οι οποίες δείχνουν το βαθμό της απειλής, της ευπάθειας και του βαθμού κινδύνου αντίστοιχα. Ο βαθμός της απειλής μπορεί να είναι Very Low(VL) , Low(L), Medium(M), High(H), Very High(VH). Ο βαθμός της ευπάθειας Low(L), Medium(M), High(H) και ο κίνδυνος από 1-7.

Πίνακας Απειλών – Αντίκτυπων

Impact / Threat	Masquerading of User Identity by Insiders	Masquerading of User Identity by CSPs	Masquerading of User Identity by Outsiders	Unauthorised Use of an Application
Physical Destruction				
Unavailability				
15 minutes	✓	✓	✓	✓
1 hour	✓	✓	✓	✓
3 hours	✓	✓	✓	✓
12 hours	✓	✓	✓	✓
1 day	✓	✓	✓	✓
2 days	✓	✓	✓	✓
1 week				
2 weeks				
1 month				
2 months				
Loss of Data since last Back-	✓	✓	✓	✓
Total Loss of all Data				
Unauthorised Disclosure				
to Insiders	✓			✓
to CSPs		✓		✓
to Outsiders			✓	✓
Small scale errors				
eg, keying errors				
in transmission				
Widespread errors				
eg, programming errors				
in transmission				
Deliberate Modification				

of Stored Data	✓	✓	✓	✓
in Transmission				
Repudiation of Origin				
Repudiation of Receipt				
Non-delivery				
Replay				
Mis-routing				
Traffic Monitoring				
Out-of-Sequence				
Insertion of False Message				

Impact / Threat	Masquerading of User Identity by Insiders	Masquerading of User Identity by CSPs	Masquerading of User Identity by Outsiders	Unauthorised Use of an Application
Physical Destruction				
Unavailability				
1 hour	✓	✓	✓	✓
3 hours	✓	✓	✓	✓
12 hours	✓	✓	✓	✓
1 day	✓	✓	✓	✓
2 days	✓	✓	✓	✓
1 week				
2 weeks				
1 month				
2 months				
Loss of Data since last Back-	✓	✓	✓	✓
Total Loss of all Data				
Unauthorised Disclosure				
to Insiders	✓			✓
to CSPs		✓		✓
to Outsiders			✓	✓
Small scale errors				
eg, keying errors				
in transmission				
Widespread errors				
eg, programming errors				
in transmission				
Deliberate Modification				
of Stored Data	✓	✓	✓	✓
in Transmission				
Repudiation of Origin				
Repudiation of Receipt				
Non-delivery				
Replay				
Mis-routing				
Traffic Monitoring				
Out-of-Sequence				
Insertion of False Message				

Impact / Threat	Introduction of Damaging or Disruptive Software	Mis-use of System Resources	Communications Infiltration	Communications Interception	Communications Manipulation
Physical Destruction					
Unavailability					
15 minutes	✓	✓	✓		
1 hour	✓	✓	✓		
3 hours	✓		✓		
12 hours	✓		✓		
1 day	✓		✓		
2 days	✓		✓		
1 week					
2 weeks					
1 month					
2 months					
Loss of Data since last Back-up	✓		✓		
Total Loss of all Data	✓				
Unauthorised Disclosure					
to Insiders	✓		✓	✓	✓
to CSPs			✓	✓	✓
to Outsiders			✓	✓	✓
Small scale errors					
eg, keying errors	✓				
in transmission	✓				✓
Widespread errors					
eg, programming errors	✓		✓		✓
in transmission	✓				✓
Deliberate Modification					
of Stored Data					
in Transmission					
Repudiation of Origin					
Repudiation of Receipt					
Non-delivery			✓		✓
Replay					✓
Mis-routing					✓
Traffic Monitoring				✓	✓
Out-of-Sequence					✓
Insertion of False Message					✓

Impact / Threat	Repudiation	Communications Failure	Embedding of Malicious Code	Accidental Misrouting
Physical Destruction				
Unavailability				
15 minutes		✓	✓	
1 hour		✓	✓	
3 hours		✓	✓	

12 hours		✓	✓	
1 day		✓	✓	
2 days		✓	✓	
1 week				
2 weeks				
1 month				
2 months				
Loss of Data since last Back-			✓	
Total Loss of all Data				
Unauthorised Disclosure				
to Insiders			✓	✓
to CSPs			✓	✓
to Outsiders			✓	✓
Small scale errors				
eg, keying errors				
in transmission				
Widespread errors				
eg, programming errors				
in transmission				
Deliberate Modification				
of Stored Data			✓	
in Transmission			✓	
Repudiation of Origin	✓			
Repudiation of Receipt	✓			
Non-delivery		✓	✓	✓
Replay			✓	
Mis-routing		✓	✓	✓
Traffic Monitoring				
Out-of-Sequence		✓	✓	
Insertion of False Message			✓	

Impact / Threat	Technical Failure of Host	Technical Failure of Storage Device	Technical Failure of Print Facilities	Technical Failure of Network Distribution Component
Physical Destruction				
Unavailability				
15 minutes	✓	✓	✓	✓
1 hour	✓	✓	✓	✓
3 hours	✓	✓	✓	✓
12 hours	✓	✓	✓	✓
1 day	✓	✓		✓
2 days	✓	✓		✓
1 week				
2 weeks				
1 month				
2 months				
Loss of Data since last Back-up	✓	✓		

Total Loss of all Data				
Unauthorised Disclosure				
to Insiders				
to CSPs				
to Outsiders				
Small scale errors				
eg, keying errors				
in transmission				
Widespread errors				
eg, programming errors				
in transmission				
Deliberate Modification				
of Stored Data				
in Transmission				
Repudiation of Origin				
Repudiation of Receipt				
Non-delivery				✓
Replay				
Mis-routing				
Traffic Monitoring				
Out-of-Sequence				✓
Insertion of False Message				

Impact / Threat	Technical Failure of Network Management / Service Host	Technical Failure of Network Interface	Failure of Network Services	Power Failure
Physical Destruction				
Unavailability				
15 minutes	✓	✓	✓	✓
1 hour	✓	✓	✓	✓
3 hours	✓	✓	✓	✓
12 hours	✓	✓	✓	✓
1 day	✓	✓	✓	✓
2 days	✓	✓	✓	✓
1 week				
2 weeks				
1 month				
2 months				
Loss of Data since last Back-up				
Total Loss of all Data				
Unauthorised Disclosure				
to Insiders				
to CSPs				
to Outsiders				
Small scale errors				
eg, keying errors				
in transmission				

Widespread errors				
eg, programming errors				
in transmission				
Deliberate Modification				
of Stored Data				
in Transmission				
Repudiation of Origin				
Repudiation of Receipt				
Non-delivery	✓	✓	✓	
Replay				
Mis-routing				
Traffic Monitoring				
Out-of-Sequence	✓			
Insertion of False Message				

Impact / Threat	Air Conditioning Failure	System or Network Software Failure	Application Software Failure	Operations Error
Physical Destruction				
Unavailability				
15 minutes	✓	✓	✓	✓
1 hour	✓	✓	✓	✓
3 hours	✓	✓	✓	✓
12 hours	✓	✓	✓	✓
1 day	✓			
2 days	✓			
1 week				
2 weeks				
1 month				
2 months				
Loss of Data since last Back-up		✓	✓	✓
Total Loss of all Data				✓
Unauthorised Disclosure				
to Insiders		✓	✓	✓
to CSPs		✓	✓	✓
to Outsiders		✓	✓	✓
Small scale errors				
eg, keying errors		✓	✓	✓
in transmission		✓	✓	✓
Widespread errors				
eg, programming errors		✓	✓	✓
in transmission		✓	✓	✓
Deliberate Modification				
of Stored Data				
in Transmission				
Repudiation of Origin				
Repudiation of Receipt				
Non-delivery		✓	✓	

Replay				
Mis-routing		✓	✓	
Traffic Monitoring				
Out-of-Sequence				
Insertion of False Message				

Impact / Threat	Hardware Maintenance Error	Software Maintenance Error	User Error	Fire
Physical Destruction				✓
Unavailability				
15 minutes	✓	✓	✓	✓
1 hour	✓	✓	✓	✓
3 hours	✓	✓		✓
12 hours	✓	✓		✓
1 day	✓			✓
2 days				✓
1 week				✓
2 weeks				✓
1 month				✓
2 months				✓
Loss of Data since last Back-up	✓	✓	✓	✓
Total Loss of all Data				
Unauthorised Disclosure				
to Insiders	✓	✓	✓	
to CSPs	✓	✓	✓	
to Outsiders	✓	✓	✓	
Small scale errors				
eg, keying errors		✓	✓	
in transmission		✓	✓	
Widespread errors				
eg, programming errors		✓		
in transmission		✓		
Deliberate Modification				
of Stored Data				
in Transmission				
Repudiation of Origin				
Repudiation of Receipt				
Non-delivery	✓	✓	✓	
Replay			✓	
Mis-routing		✓	✓	
Traffic Monitoring				
Out-of-Sequence			✓	
Insertion of False Message				

Impact / Threat	Water Damage	Natural Disaster	Staff Shortage	Theft by Insiders
Physical Destruction	✓	✓		✓

Unavailability				
15 minutes	✓	✓	✓	✓
1 hour	✓	✓	✓	✓
3 hours	✓	✓	✓	✓
12 hours	✓	✓	✓	✓
1 day	✓	✓	✓	✓
2 days	✓	✓	✓	✓
1 week	✓	✓	✓	✓
2 weeks		✓		
1 month		✓		
2 months		✓		
Loss of Data since last Back-up	✓	✓		✓
Total Loss of all Data				
Unauthorised Disclosure				
to Insiders			✓	✓
to CSPs			✓	✓
to Outsiders			✓	✓
Small scale errors				
eg, keying errors				
in transmission				
Widespread errors				
eg, programming errors				
in transmission				
Deliberate Modification				
of Stored Data			✓	
in Transmission			✓	
Repudiation of Origin				
Repudiation of Receipt				
Non-delivery				
Replay				
Mis-routing				
Traffic Monitoring				
Out-of-Sequence				
Insertion of False Message				

Impact / Threat	Theft by Outsiders	Wilful Damage by Insiders	Wilful Damage by Outsiders	Military Action / Terrorism
Physical Destruction	✓	✓	✓	✓
Unavailability				
15 minutes	✓	✓	✓	✓
1 hour	✓	✓	✓	✓
3 hours	✓	✓	✓	✓
12 hours	✓	✓	✓	✓
1 day	✓	✓	✓	✓
2 days	✓	✓	✓	✓
1 week	✓	✓	✓	✓
2 weeks				✓
1 month				✓

2 months				✓
Loss of Data since last Back-up	✓	✓	✓	✓
Total Loss of all Data		✓		✓
Unauthorised Disclosure				
to Insiders	✓			
to CSPs	✓			
to Outsiders	✓			
Small scale errors				
eg, keying errors				
in transmission				
Widespread errors				
eg, programming errors				
in transmission				
Deliberate Modification				
of Stored Data				
in Transmission				
Repudiation of Origin				
Repudiation of Receipt				
Non-delivery				
Replay				
Mis-routing				
Traffic Monitoring				
Out-of-Sequence				
Insertion of False Message				

Πίνακας Αποτίμησης Απειλών – Ευπαθειών

	Threat	**Vulnerability**
Masquerading of User Identity by Insiders / Outsiders		
Medical Data	Medium	Medium
Personal Data	Medium	Medium
Patient Management Data	Medium	Medium
Clinical Protocols	Low	Medium
Data Indexes for Integrating Processes	Medium	Low
Financial/Logistics	Medium	High
MIS Data – BI Data	Low	Low
Administrative Data	Medium	High
Systems Data	Medium	Medium
Communication Infiltration		
Medical Data	Medium	Medium
Personal Data	High	Medium
Patient Management Data	Low	Low
Clinical Protocols	Low	Medium
Data Indexes for Integrating Processes	Medium	Medium
Financial/Logistics	Medium	High
MIS Data – BI Data	Low	Low

Administrative Data	Medium	High
Systems Data	Medium	Medium
Communication Interception		
Medical Data	Medium	Medium
Personal Data	Low	Low
Patient Management Data	Very Low	Medium
Clinical Protocols	Very Low	Medium
Data Indexes for Integrating Processes	Very Low	Low
Financial/Logistics	Medium	High
MIS Data – BI Data	Low	Low
Administrative Data	Very High	Medium
Systems Data	Medium	Medium
Communication Manipulation		
Medical Data	Low	Medium
Personal Data	Very Low	Low
Patient Management Data	Low	Low
Clinical Protocols	Very Low	Low
Data Indexes for Integrating Processes	Very Low	Low
Financial/Logistics	High	High
MIS Data – BI Data	Low	Low
Administrative Data	Very High	High
Systems Data	Low	Low
Communication Failure		
Medical Data	Medium	High
Personal Data	Medium	Medium
Patient Management Data	High	High
Clinical Protocols	Medium	Medium
Data Indexes for Integrating Processes	Medium	Medium
Financial/Logistics	Medium	Low
MIS Data – BI Data	Low	Low
Administrative Data	High	Low
Systems Data	High	Low
Repudiation		
Medical Data	Low	Low
Personal Data	Medium	Low
Patient Management Data	High	Medium
Clinical Protocols	High	Low
Data Indexes for Integrating Processes	High	Medium
Financial/Logistics	Medium	Medium
MIS Data – BI Data	Low	Low
Administrative Data	High	Medium
Systems Data	Medium	Low
Accidental Misrouting		
Medical Data	High	High

Personal Data	Very High	High
Patient Management Data	Very High	High
Clinical Protocols	Medium	Medium
Data Indexes for Integrating Processes	Low	Medium
Financial/Logistics	High	Medium
MIS Data – BI Data	Medium	Low
Administrative Data	High	High
Systems Data	Medium	Medium
Theft by Insiders / Outsiders		
Medical Data	Medium	High
Personal Data	High	High
Patient Management Data	Medium	Low
Clinical Protocols	Low	Low
Data Indexes for Integrating Processes	Very Low	Low
Financial/Logistics	Medium	Low
MIS Data – BI Data	Medium	Medium
Administrative Data	Medium	Medium
Systems Data	High	Medium
Application Network Server	Medium	High
Printers	Very Low	Low
Backup Media	Low	Low
Backup Server	Very Low	Low
DNS Server	Very Low	Low
Authentication Server	Very Low	Low
Database Server	Very Low	Low
System or Network Software Failure		
Medical Data	Medium	High
Personal Data	Medium	Medium
Patient Management Data	High	Medium
Clinical Protocols	Very Low	Low
Data Indexes for Integrating Processes	Medium	Low
Financial/Logistics	Medium	Medium
MIS Data – BI Data	High	Low
Administrative Data	High	Medium
Systems Data	Low	Low
Application Network Server	Medium	Medium
Printers	High	Low
Backup Media	Low	Low
Backup Server	Medium	Low
DNS Server	Medium	Medium
Authentication Server	Medium	Medium
Database Server	High	High
Medical Record Software	High	High
Patient Telemonitoring Support	Medium	High
Logging Support Software	Medium	Medium
Teleconference Support Software	Low	Low
Database Transaction Software	Medium	Medium

Introduction of Damaging or Disruptive Software		
Medical Data	High	High
Personal Data	High	Medium
Patient Management Data	High	Medium
Clinical Protocols	Very Low	Low
Data Indexes for Integrating Processes	Low	Low
Financial/Logistics	Medium	Low
MIS Data – BI Data	Low	Medium
Administrative Data	Medium	Medium
Systems Data	Very Low	Low
Medical Record Software	High	High
Patient Telemonitoring Support	Low	Medium
Logging Support Software	Medium	Low
Teleconference Support Software	Medium	Medium
Database Transaction Software	High	High
Embedding of Malicious Code		
Medical Data	High	High
Personal Data	High	Medium
Patient Management Data	High	Medium
Clinical Protocols	Very Low	Low
Data Indexes for Integrating Processes	Low	Low
Financial/Logistics	Medium	Low
MIS Data – BI Data	Low	Medium
Administrative Data	Medium	Medium
Systems Data	Very Low	Low
Medical Record Software	High	High
Patient Telemonitoring Support	Low	Medium
Logging Support Software	Medium	Low
Teleconference Support Software	Medium	Medium
Database Transaction Software	High	High
Technical Failure of Host		
Medical Data	Medium	High
Personal Data	Medium	Medium
Patient Management Data	High	Medium
Clinical Protocols	Very Low	Low
Data Indexes for Integrating Processes	Medium	Low
Financial/Logistics	Medium	Medium
MIS Data – BI Data	High	Low
Administrative Data	High	Medium
Systems Data	Low	Low
Application Network Server	Low	Low
Printers	Low	Low
Backup Media	Low	Low
Backup Server	Low	Low
DNS Server	Low	Low
Authentication Server	Low	Low

Database Server	Low	Low
Technical Failure of Storage Device		
Medical Data	Medium	Medium
Personal Data	Low	Low
Patient Management Data	Low	Low
Clinical Protocols	Low	Low
Data Indexes for Integrating Processes	Medium	Medium
Financial/Logistics	Medium	Low
MIS Data – BI Data	Medium	Low
Administrative Data	Medium	Low
Systems Data	Low	Low
Backup Media	Low	Low
Application Software Failure		
Medical Data	High	High
Personal Data	Medium	Medium
Patient Management Data	Very High	Medium
Clinical Protocols	Very Low	Low
Data Indexes for Integrating Processes	High	Medium
Financial/Logistics	Very High	Medium
MIS Data – BI Data	High	Medium
Administrative Data	Medium	Medium
Systems Data	Low	Low
Medical Record Software	High	High
Patient Telemonitoring Support	High	HIgh
Logging Support Software	High	Medium
Teleconference Support Software	Medium	Low
Database Transaction Software	High	Medium
Operations Error		
Medical Data	High	High
Personal Data	High	HIgh
Patient Management Data	High	Medium
Clinical Protocols	Very High	High
Data Indexes for Integrating Processes	Medium	Medium
Financial/Logistics	High	Medium
MIS Data – BI Data	Medium	Medium
Administrative Data	Medium	Medium
Systems Data	Low	Low
Application Network Server	Medium	Low
Printers	Medium	Low
Backup Media	Low	Low
Backup Server	Medium	Low
DNS Server	Medium	Low
Authentication Server	Medium	Medium
Database Server	Medium	Medium
Medical Record Software	High	High
Patient Telemonitoring Support	High	High

Logging Support Software	Medium	Medium
Teleconference Support Software	Low	Low
Database Transaction Software	Medium	Medium
Staff Shortage		
Medical Data	Medium	Medium
Personal Data	Medium	Medium
Patient Management Data	Medium	Low
Clinical Protocols	Low	Low
Data Indexes for Integrating Processes	Very Low	Low
Financial/Logistics	Low	Low
MIS Data – BI Data	Low	Low
Administrative Data	Low	Low
Systems Data	Very Low	Low
User Error		
Medical Data	High	High
Personal Data	High	High
Patient Management Data	High	Medium
Clinical Protocols	Low	Medium
Data Indexes for Integrating Processes	Medium	Medium
Financial/Logistics	High	Medium
MIS Data – BI Data	Medium	Medium
Administrative Data	Medium	Medium
Systems Data	Low	Low
Medical Record Software	High	High
Patient Telemonitoring Support	High	High
Logging Support Software	Medium	Medium
Teleconference Support Software	Low	Low
Database Transaction Software	Medium	Medium
Application Network Server	Low	Low
Printers	Very Low	Low
Backup Media	Very Low	Low
Backup Server	Medium	Low
DNS Server	Low	Low
Authentication Server	Low	Low
Database Server	Low	Low
Medical Record Software	Very Low	Low
Patient Telemonitoring Support	Very Low	Low
Logging Support Software	Very Low	Medium
Teleconference Support Software	Medium	Low
Database Transaction Software	Very Low	Low
Misuse of System's Resources		
Application Network Server	Very Low	Medium
Printers	Low	Low
Backup Media	Low	Low
Backup Server	Low	High
DNS Server	Very Low	Medium

Authentication Server	Very Low	Medium
Database Server	Very Low	Medium
Medical Record Software	Very Low	Low
Patient Telemonitoring Support	Very Low	Low
Logging Support Software	Very Low	Medium
Teleconference Support Software	Medium	Low
Database Transaction Software	Very Low	Low
Willful Damage		
Application Network Server	High	Low
Printers	High	Low
Backup Media	High	Low
Backup Server	High	Low
DNS Server	High	Low
Authentication Server	High	Low
Database Server	High	Low
Power Failure		
Application Network Server	Medium	Medium
Printers	Low	Low
Backup Media	Low	Medium
Backup Server	Medium	Medium
DNS Server	Medium	Medium
Authentication Server	Medium	Medium
Database Server	Medium	Medium
Hardware Maintenance Error		
Application Network Server	Medium	Medium
Printers	Low	Low
Backup Media	Low	Medium
Backup Server	Medium	Medium
DNS Server	Medium	Medium
Authentication Server	Medium	Medium
Database Server	Medium	Medium
Technical Failure of Print Device		
Printers	High	High
Technical Failure of Network Distribution Components		
Application Network Server	Medium	Medium
Printers	Very Low	Low
Backup Media	Very Low	Low
Backup Server	Medium	Medium
DNS Server	Medium	Medium
Authentication Server	Medium	Medium
Database Server	Medium	Medium
Unauthorized Use of an Application		
Medical Data	High	High

Personal Data	Very High	High
Patient Management Data	High	Medium
Clinical Protocols	Medium	Medium
Data Indexes for Integrating Processes	Low	Low
Financial/Logistics	Low	Low
MIS Data – BI Data	Very Low	Low
Administrative Data	Medium	Low
Systems Data	Very Low	Low
Medical Record Software	High	High
Patient Telemonitoring Support	Very Low	Low
Logging Support Software	Low	Low
Teleconference Support Software	Very Low	Low
Database Transaction Software	Medium	Medium
Technical Failure of Network Interface		
Medical Record Software	High	High
Patient Telemonitoring Support	High	High
Logging Support Software	High	Medium
Teleconference Support Software	High	Low
Database Transaction Software	High	High
Technical Failure of Network Services		
Application Network Server	Medium	Medium
Printers	High	Low
Backup Media	Low	Low
Backup Server	Medium	Low
DNS Server	Medium	Medium
Authentication Server	Medium	Medium
Database Server	High	High
Medical Record Software	High	High
Patient Telemonitoring Support	High	High
Logging Support Software	High	Medium
Teleconference Support Software	High	Low
Database Transaction Software	High	High
Software Maintenance Error		
Medical Record Software	Medium	High
Patient Telemonitoring Support	Medium	High
Logging Support Software	Low	Low
Teleconference Support Software	High	Low
Database Transaction Software	Medium	High

Πίνακας Αναλυτικών Αποτελεσμάτων Βαθμού Κινδύνου

	Threat	**Vulnerability**	**MoR**
Masquerading of user identity by insiders-outsiders			
Medical Data	Medium	Medium	6

Personal Data	Medium	Medium	5
Patient Management Data	Medium	Medium	4
Clinical Protocols	Low	Medium	3
Data Indexes for Integrating Processes	Medium	Low	3
Financial/Logistics	Medium	High	5
MIS Data – BI Data	Low	Low	3
Administrative Data	Medium	High	5
Systems Data	Medium	Medium	3
Communications infiltration			
Medical Data	Medium	Medium	6
Personal Data	High	Medium	6
Patient Management Data	Low	Low	3
Clinical Protocols	Low	Medium	3
Data Indexes for Integrating Processes	Medium	Medium	4
Financial/Logistics	Medium	High	5
MIS Data – BI Data	Low	Low	3
Administrative Data	Medium	High	5
Systems Data	Medium	Medium	3
Communication Interception			
Medical Data	Medium	Medium	6
Personal Data	Low	Low	4
Patient Management Data	Very Low	Medium	3
Clinical Protocols	Very Low	Medium	3
Data Indexes for Integrating Processes	Very Low	Low	2
Financial/Logistics	Medium	High	5
MIS Data – BI Data	Low	Low	3
Administrative Data	Very High	Medium	5
Systems Data	Medium	Medium	3
Communication Manipulation			
Medical Data	Low	Medium	6
Personal Data	Very Low	Low	4
Patient Management Data	Low	Low	3
Clinical Protocols	Very Low	Low	2
Data Indexes for Integrating Processes	Very Low	Low	2
Financial/Logistics	High	High	5
MIS Data – BI Data	Low	Low	3
Administrative Data	Very High	High	6
Systems Data	Low	Low	2
Communication Failure			
Medical Data	Medium	High	6
Personal Data	Medium	Medium	5
Patient Management Data	High	High	5
Clinical Protocols	Medium	Medium	4
Data Indexes for Integrating Processes	Medium	Medium	4
Financial/Logistics	Medium	Low	4

MIS Data – BI Data	Low	Low	3
Administrative Data	High	Low	4
Systems Data	High	Low	3
Repudiation			
Medical Data	Low	Low	5
Personal Data	Medium	Low	5
Patient Management Data	High	Medium	5
Clinical Protocols	High	Low	4
Data Indexes for Integrating Processes	High	Medium	4
Financial/Logistics	Medium	Medium	4
MIS Data – BI Data	Low	Low	3
Administrative Data	High	Medium	5
Systems Data	Medium	Low	3
Accidental Misrouting			
Medical Data	High	High	7
Personal Data	Very High	High	7
Patient Management Data	Very High	High	6
Clinical Protocols	Medium	Medium	4
Data Indexes for Integrating Processes	Low	Medium	3
Financial/Logistics	High	Medium	5
MIS Data – BI Data	Medium	Low	3
Administrative Data	High	High	5
Systems Data	Medium	Medium	3
Theft by Insiders/Outsiders			
Medical Data	Medium	High	6
Personal Data	High	High	6
Patient Management Data	Medium	Low	4
Clinical Protocols	Low	Low	3
Data Indexes for Integrating Processes	Very Low	Low	2
Financial/Logistics	Medium	Low	4
MIS Data – BI Data	Medium	Medium	4
Administrative Data	Medium	Medium	4
Systems Data	High	Medium	4
Application Network Server	Medium	High	4
Printers	Very Low	Low	1
Backup Media	Low	Low	1
Backup Server	Very Low	Low	1
DNS Server	Very Low	Low	1
Authentication Server	Very Low	Low	1
Database Server	Very Low	Low	1
System / Network Software Failure			
Medical Data	Medium	High	6
Personal Data	Medium	Medium	5
Patient Management Data	High	Medium	5
Clinical Protocols	Very Low	Low	2

Data Indexes for Integrating Processes	Medium	Low	3
Financial/Logistics	Medium	Medium	4
MIS Data – BI Data	High	Low	4
Administrative Data	High	Medium	5
Systems Data	Low	Low	2
Application Network Server	Medium	Medium	3
Printers	High	Low	2
Backup Media	Low	Low	1
Backup Server	Medium	Low	2
DNS Server	Medium	Medium	2
Authentication Server	Medium	Medium	2
Database Server	High	High	3
Medical Record Software	High	High	3
Patient Telemonitoring Support	Medium	High	3
Logging Support Software	Medium	Medium	2
Teleconference Support Software	Low	Low	1
Database Transaction Software	Medium	Medium	2
Introduction of Damaging / Disruptive Software			
Medical Data	High	High	7
Personal Data	High	Medium	6
Patient Management Data	High	Medium	5
Clinical Protocols	Very Low	Low	2
Data Indexes for Integrating Processes	Low	Low	3
Financial/Logistics	Medium	Low	4
MIS Data – BI Data	Low	Medium	3
Administrative Data	Medium	Medium	4
Systems Data	Very Low	Low	2
Medical Record Software	High	High	3
Patient Telemonitoring Support	Low	Medium	2
Logging Support Software	Medium	Low	2
Teleconference Support Software	Medium	Medium	1
Database Transaction Software	High	High	3
Embedding of Malicious Code			
Medical Data	High	High	7
Personal Data	High	Medium	6
Patient Management Data	High	Medium	5
Clinical Protocols	Very Low	Low	2
Data Indexes for Integrating Processes	Low	Low	3
Financial/Logistics	Medium	Low	4
MIS Data – BI Data	Low	Medium	3
Administrative Data	Medium	Medium	4
Systems Data	Very Low	Low	2
Medical Record Software	High	High	3
Patient Telemonitoring Support	Low	Medium	2
Logging Support Software	Medium	Low	2
Teleconference Support Software	Medium	Medium	1
Database Transaction Software	High	High	3

Technical Failure of Host			
Medical Data	Medium	High	6
Personal Data	Medium	Medium	5
Patient Management Data	High	Medium	5
Clinical Protocols	Very Low	Low	2
Data Indexes for Integrating Processes	Medium	Low	3
Financial/Logistics	Medium	Medium	4
MIS Data – BI Data	High	Low	4
Administrative Data	High	Medium	5
Systems Data	Low	Low	2
Application Network Server	Low	Low	2
Printers	Low	Low	1
Backup Media	Low	Low	1
Backup Server	Low	Low	2
DNS Server	Low	Low	1
Authentication Server	Low	Low	1
Database Server	Low	Low	1
Technical Failure of Storage Device			
Medical Data	Medium	Medium	6
Personal Data	Low	Low	4
Patient Management Data	Low	Low	3
Clinical Protocols	Low	Low	3
Data Indexes for Integrating Processes	Medium	Medium	4
Financial/Logistics	Medium	Low	4
MIS Data – BI Data	Medium	Low	3
Administrative Data	Medium	Low	4
Systems Data	Low	Low	2
Backup Media	Low	Low	1
Application Software Failure			
Medical Data	High	High	7
Personal Data	Medium	Medium	5
Patient Management Data	Very High	Medium	5
Clinical Protocols	Very Low	Low	2
Data Indexes for Integrating Processes	High	Medium	4
Financial/Logistics	Very High	Medium	5
MIS Data – BI Data	High	Medium	4
Administrative Data	Medium	Medium	4
Systems Data	Low	Low	2
Medical Record Software	High	High	3
Patient Telemonitoring Support	High	HIgh	3
Logging Support Software	High	Medium	3
Teleconference Support Software	Medium	Low	1
Database Transaction Software	High	Medium	3
Operations Error			
Medical Data	High	High	7

Personal Data	High	HIgh	6
Patient Management Data	High	Medium	6
Clinical Protocols	Very High	High	6
Data Indexes for Integrating Processes	Medium	Medium	4
Financial/Logistics	High	Medium	5
MIS Data – BI Data	Medium	Medium	4
Administrative Data	Medium	Medium	4
Systems Data	Low	Low	2
Application Network Server	Medium	Low	2
Printers	Medium	Low	2
Backup Media	Low	Low	1
Backup Server	Medium	Low	2
DNS Server	Medium	Low	2
Authentication Server	Medium	Medium	2
Database Server	Medium	Medium	2
Medical Record Software	High	High	3
Patient Telemonitoring Support	High	High	3
Logging Support Software	Medium	Medium	2
Teleconference Support Software	Low	Low	1
Database Transaction Software	Medium	Medium	2
Staff Shortage			
Medical Data	Medium	Medium	6
Personal Data	Medium	Medium	5
Patient Management Data	Medium	Low	4
Clinical Protocols	Low	Low	3
Data Indexes for Integrating Processes	Very Low	Low	2
Financial/Logistics	Low	Low	3
MIS Data – BI Data	Low	Low	3
Administrative Data	Low	Low	3
Systems Data	Very Low	Low	2
User Error			
Medical Data	High	High	7
Personal Data	High	High	6
Patient Management Data	High	Medium	6
Clinical Protocols	Low	Medium	3
Data Indexes for Integrating Processes	Medium	Medium	4
Financial/Logistics	High	Medium	5
MIS Data – BI Data	Medium	Medium	4
Administrative Data	Medium	Medium	4
Systems Data	Low	Low	2
Medical Record Software	High	High	3
Patient Telemonitoring Support	High	High	3
Logging Support Software	Medium	Medium	2
Teleconference Support Software	Low	Low	1
Database Transaction Software	Medium	Medium	2
Misuse of System's Resources			

Application Network Server	Low	Low	2
Printers	Very Low	Low	1
Backup Media	Very Low	Low	1
Backup Server	Medium	Low	2
DNS Server	Low	Low	1
Authentication Server	Low	Low	1
Database Server	Low	Low	1
Medical Record Software	Very Low	Low	1
Patient Telemonitoring Support	Very Low	Low	1
Logging Support Software	Very Low	Medium	1
Teleconference Support Software	Medium	Low	1
Database Transaction Software	Very Low	Low	1
Willful Damage			
Application Network Server	Very Low	Medium	2
Printers	Low	Low	1
Backup Media	Low	Low	1
Backup Server	Low	High	3
DNS Server	Very Low	Medium	1
Authentication Server	Very Low	Medium	1
Database Server	Very Low	Medium	1
Power Failure			
Application Network Server	High	Low	3
Printers	High	Low	2
Backup Media	High	Low	3
Backup Server	High	Low	2
DNS Server	High	Low	2
Authentication Server	High	Low	2
Database Server	High	Low	2
Hardware Maintenance Error			
Application Network Server	Medium	Medium	3
Printers	Low	Low	1
Backup Media	Low	Medium	2
Backup Server	Medium	Medium	3
DNS Server	Medium	Medium	2
Authentication Server	Medium	Medium	2
Database Server	Medium	Medium	2
Technical Failure of Print Device			
Printers	High	High	3
Technical Failure of Network Distribution Components			
Application Network Server	Medium	Medium	3
Printers	Very Low	Low	1
Backup Media	Very Low	Low	1
Backup Server	Medium	Medium	3
DNS Server	Medium	Medium	2

Authentication Server	Medium	Medium	2
Database Server	Medium	Medium	2
Unauthorized Use of an Application			
Medical Data	High	High	7
Personal Data	Very High	High	7
Patient Management Data	High	Medium	5
Clinical Protocols	Medium	Medium	4
Data Indexes for Integrating Processes	Low	Low	3
Financial/Logistics	Low	Low	3
MIS Data – BI Data	Very Low	Low	2
Administrative Data	Medium	Low	4
Systems Data	Very Low	Low	2
Medical Record Software	High	High	3
Patient Telemonitoring Support	Very Low	Low	1
Logging Support Software	Low	Low	1
Teleconference Support Software	Very Low	Low	1
Database Transaction Software	Medium	Medium	2
Technical Failure of Network Interface			
Medical Record Software	High	High	3
Patient Telemonitoring Support	High	High	3
Logging Support Software	High	Medium	3
Teleconference Support Software	High	Low	1
Database Transaction Software	High	High	3
Technical Failure of Network Services			
Application Network Server	Medium	Medium	3
Printers	High	Low	2
Backup Media	Low	Low	1
Backup Server	Medium	Low	2
DNS Server	Medium	Medium	2
Authentication Server	Medium	Medium	2
Database Server	High	High	3
Medical Record Software	High	High	3
Patient Telemonitoring Support	High	High	3
Logging Support Software	High	Medium	3
Teleconference Support Software	High	Low	1
Database Transaction Software	High	High	3
Software Maintenance Error			
Medical Record Software	Medium	High	3
Patient Telemonitoring Support	Medium	High	3
Logging Support Software	Low	Low	1
Teleconference Support Software	High	Low	1
Database Transaction Software	Medium	High	3

Βιβλιογραφικές Παραπομπές

Ελληνική Βιβλιογραφία

Αποστολάκης, Ι., (2002), «*Πληροφοριακά Συστήματα Υγείας»*, Εκδόσεις Παπαζήση, Αθήνα.

Βαγγελάτος, Α. Σαριβουγιούκας, Ι. (2002a). Πληροφοριακό Σύστημα Νοσοκομείου: Απαραίτητη Υποδομή στο Σύγχρονο Νοσοκομείο. Ιατρική 2001, Νο 9. Εταιρεία Ιατρικών Σπουδών. Εκδόσεις ΒΗΤΑ.

Γρίβας Β., Κουκούμας Ν., Ξανθόπουλος Κ., Σφυρής Ν., Χρυσοχοίδης Ι., "Οικονομική και Χρηματοδοτική Διαχείριση Υπηρεσιών Υγείας", Ελληνικό Ανοικτό Πανεπιστήμιο.

Κατσίκας Σ., Risk Analysis and Risk Management: Capabilities and Limitations

Κίτσιου, Σ., (2010), Διπλωματική Εργασία «Πληροφοριακά Συστήματα στο Χώρο της Υγείας: Ανάπτυξη Μοντέλου Συγκριτικής Αξιολόγησης και Διεξαγωγή Πανελλαδικής Έρευνας για την Επιμέτρηση του Βαθμού Υιοθέτησης και Εξέλιξης των Πληροφοριακών Συστημάτων στα Δημόσια Νοσοκομεία» , Αυτοέκδοση.

Κίτσιου, Σ., Βλαχοπούλου, Μ., (2008), «η-Υγεία: Πληροφοριακά Συστήματα και Ηλεκτρονικές Υπηρεσίες στο χώρο της Υγείας», Εκδοτικός Οίκος Πανεπιστημίου Μακεδονίας, Θεσσαλονίκη.

Πάγκαλος Γ. και Μαυρίδης Ι., Ασφάλεια Πληροφοριακών συστημάτων, ΑΝΙΚΟΥΛΑ

Παπουτσής, Ι. Παπαδημητρίου, Ι. (1999). Ηλεκτρονικός ιατρικός φάκελος ασθενών. Υλοποίηση στο Αρεταίειο Πανεπιστημιακό νοσοκομείο. Ιατρική 1999, 75 (1):64-70 .

Υπουργείο Ανάπτυξης, Ε.Π. Κοινωνία της Πληροφορίας, Τελικό Παραδοτέο Ομάδας Ζ3 με θέμα: «Διαλειτουργικότητα Πληροφοριακών Συστημάτων στην Υγεία – Πρόνοια και Κοινωνική Ασφάλιση: Προοπτικές και Ανάγκες Τελικών Χρηστών,» ebusinessforum.

Ξένη Βιβλιογραφία

A. Appari and M. E. Johnson, "Information Security and Privacy in Healthcare: Current State of Research," *International Journal of Internet and Enterprise Management*, Vol. 6, No. 4, 2010, pp. 279-314.

Agrawal, R., & Johnson, C (2007). 'Securing Electronic Health Records without impeding the flow of information. *International Journal of Medical Informatics,* 76 (5-6), 471-479.

Anderson, J. G. (2007). Social, Ethical and Legal Barriers to E-Health. . *International Journal of Medical Informatics,* 76 (5-6), 480-483.

Bill Vargas, Pradeep Ray, —Interoperability of Hospital Information Systems: A Case Study, University of New South Wales, Australia, IEEE 2003

Blobel, B. (2000). Application of the component paradigm for analysis and design of advanced health systems architectures. *International Journal of Medical Informatics,* 60(3), 281-301.

Blobel, B. (2004). Authorization and access control for electronic health record systems. *International Journal of Medical Informatics,* 73(3), 251-257.

Blobel, B. (2006a). Advanced and secure architectural EHR approaches. *International Journal of Medical Informatics,* 75(3-4), 185-190.

Blobel, B., & Roger-France, F. (2001). A systematic approach for analysis and design of secure health information systems. *International Journal of Medical Informatics,* 62(1), 51-78.

Brender, J., Ammenwerth, E., Nykanen, P., Talmon, J., (2006). "Factors Influencing Success and Failure of Health Informatics Systems - A Pilot Delphi Study", Methods of Information in Medicine, Vol. 45, pp. 125-136.

Choe , J., & Yoo, S. K. (2008). Web-based Secure access from multiple patient repositories. *International Journal of Medical Informatics,* 77(4), 242-248.

Collen, M.F. (1974). (ed). Hospital Computer Systems. New York: John Wiley & Sons, 1974.

Conrick, M., & Newell, C. (2006). Issues of Ethics and Law. In M. Conrick (Ed.), *Health Informatics: Transforming Healthcare with Technology.* Melbourne: Social Science Press.

Cramm User Guide, Issue 5.1, (2005).

D. Gritzalis, S. Katsikas, J. Keklikoglou, A. Tomaras, Determining access rights for medical information systems, Computers & Security 11 (1992) 149–161.

D. Kotz, “A Threat Taxonomy for mHealth Privacy,” *Proceedings of the 3rd International Conference on Com- munication Systems and Networks of the IEEE COMS- NETS*, Bangalore, 4-8 January 2011, pp. 1-6.

G.J. Pangalos, Medical Database Security Policies, In: J.H. Van Bemmel, A.T. McCray, Yearbook ’94 of Medical Informatics. Advanced communications in health-care, Schattauer IMIA, p. 253–259.

Grimson, J. Grimson, W. Hasselbring, W. (2000). “The SI Challenge in Health Care, Communications of the ACM”, Volume 43, Number 6, 48-55.

Gritzalis, D., & Lamprinoudakis, C. (2004). A security architecture for interconnecting health information systems. *International Journal of Medical Informatics,* 73(3), 305-309.

Hammond, W.E. (1994). Hospital information system: a review in perspective, Yearbook Med. Inf. 95/102.

Hasselbring, W. (1999). On Defining Computer Science Terminology. COMMUNICATIONS OF THE ACM, February 1999/Vol. 42, No. 2.

Haux, R. (2006b). Individualization globalization and health – about sustainable information technologies and the aim of medical informatics, 75(12), 795-808.

HL7, Health Level Seven: An application protocol for electronic data exchange in healthcare environments. Version 2.1 1990. Chicago, Ill.: Health Level Seven, Inc, 1990.

"Information Security Risk Assessment, Practices of Leading Organizations", GAO/AIMD-99-139, United States General Accounting Office, 1999.

J. H. Pardue and P. Patidar, "Thrats to Healthcare Date: A Threat Tree for Risk Assessment," *Issues in Information Systems*, 5-8 October 2011.

J. P. Landry, et al., "A Threat Tree for Health Information Security and Privacy," Proceedings of the 17th American Conference on Information Systems, Detroit, 4-8 August 2011.

Junghans, G. (1995). Network communication and Management in a HIS-Environment, in: Prokosch, H. U. Dudeck, J. Hospital Information Systems a Pragmatic Definition, Elsevier.

Kazanjian, A. Pagliccia, N. (1998). Health Decision Support Systems for technology assessment: Toward a Decision Model of Health Technology Diffusion. Health Decision Support Systems, ASPEN Publisher, Inc. 1998.

M. E. Whitman and H. J. Mattord, "Principles of Infor-mation Security," Course Technology Ptr, Boston, 2011.

Maglogiannis, I., Zafeiropoulos, I., 'Modeling Risk in Distributed Healthcare Information Systems'.

Meingast, M., Roosta, T., Sastry, S. (2006), 'Security and Privacy Issues with health care Information Technology', Annual International Conference, vol. 28.

Mohd, M., Y., Anastasia Papazafeiropoulou, Paul, R., J., Stergioulas, L., K., (2008), "Investigating Evaluation Framworks for Health Information Systems", Elsevier, International Journal of Medical Informatics Vol. 77, pp 377-385.

Mulligen, E. M. Timmers, T. Bemmel, J.H. Heuvel F. (1992). Functional Requirements for an Integrated Medical Workstation. Proceedings World Congress Medical Informatics, Geneva, North Holland 1261.

Nichols A., A Perspective on Threats in the Risk Analysis Process, SANS Institute, 2002.

Ozbolt, J. G. Bakken, S. (2001). Patient care systems, in: E.H. Shortliffe, L.E. Perreault(Eds.), Medical Informatics: “Computer Applications in Health Care and Biomedicine”, 2nd ed., Springer, New York, 2001, pp. 421/422.

P. Doupi et.al. “Implementing interoperable secure health information systems”, Regional Health Economies and ICT services, pp 187-214, IOS Press 2005, ISBN.

Peristeras, V., Tarabanis, K., (2006). ‘The Connection, Communication, Consolidation, Collaboration Interoperability Framework (C4IF) For Information Systems Interoperability,’ *Interoperability in Business Information Systems,* 1(1) 61-72.

Peterson, H.E. Gerdin-Jelger, U. (1988). The history of hospital information systems. 3:241- 217.

Prokosch, H.U. (1995) Hospital Information Systems: A Pragmatic Definition, in: Prokosch, H. U. Dudeck, J. Hospital Information Systems a Pragmatic Definition, Elsevier.

Russell-Richard Swansburg, “Εισαγωγή στη νοσηλευτική διοίκηση και ηγεσία”, Ιατρικές Εκδόσεις.

Sicotte et. al. “ A Risk Assessment of Two Interorganizational Clinical Information Systems”, JAMIA, vol. 13, No 5, pp 557-566.

Scherrer, J. R. Baud, R. Roulet, D. (1995). Moving towards the future design of HIS: a view from the Seventies to the End of the Nineties, the DIOGENE Paradigm. in: Prokosch, H. U. Dudeck, J. Hospital Information Systems a Pragmatic Definition, Elsevier.

Smith, E., Eloff, J.H.P., (1998), ‘Security in healthcare Information Sytems,’ *International Journal of Medical Informatic,* 54 (1999) 39–54.

Smith, J. (2000) Health management Information Systems. A Handbook for decision makers. Open University Press, Buckingham, Philadelphia.

Spyrou, S. S., Bamidis, P., Chouvarda, I., Gogou, G., Tryfon, S.M., and Maglaveras, N., (2002). ‘Healthcare Informatics Standards: Comparison of the Approaches,’ *Health Informatics Journal*, 8(1), 14-19.

Standards for E-Health Interoperability, Andrew Goodchild, National E-Health Transition Authority

T. C. Rindfleisch, “Privacy, Information Technology, and Health Care,” *Communications of the ACM*, Vol. 40, No. 8, 1997, pp. 92 100.

Tan, J., Raghupathi, W. (2002). Strategic IT applications in health care. Communications of the ACM, Volume 45 Issue 12.

WHO (2006). “Health information systems in support of the Millennium Development”. Goals Report by the Secretariat, SIXTIETH WORLD HEALTH ASSEMBLY A60/22.

Wilcox, A., Kuperman, G., Dorr, D. A., Hripcsak, G., Narus, S. P., Thornton, S. N., and Evans, R.S., (2003). ‘ Architectural strategies and issues with health information exchange,’ AMIA Annu Symp, Proc, pp, 814-8.

Zviran, M. (1990). “Defining the application portofolio for an integrated hospital management information system”. Journal of Medical Systems, 14 (1/2), pp31-41

Ηλεκτρονική Βιβλιογραφία

http://www.ccs.gr/iatrikh/proionta/e-AIMA/index.asp

http://www.kyanousstavros.gr/

Ευρωπαϊκή Οδηγία 95/46/EC. http://ec.europa.eu/justice/data-protection/index_en.htm

Καρπουζής, Κ., (2004), «Ηλεκτρονικές Υπηρεσίες υγείας», WWW] Available from: http://dtps.unipi.gr/files/notes/2004-2005/eksamino_7/ hlektronikes_yphresies_ ygeias/ ehealth04.ppt.

Νομοθετικό πλαίσιο που προνοεί για το νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές http://www.steadlands.com/interlink/pdfs/legislation/cyprus.pdf]

Ο Χάρτης των Θεμελιωδών Δικαιωμάτων http://www.europarl.europa.eu/portal/en

Οδηγία 95/46/ΕΚ http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=el&type_doc=Directive&an_doc=1995&nu_doc=46]

Οδηγία 2002/58/ΕΚ http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=2002&nu_doc=58]

Οδηγία 1999/5/ΕΚ https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=276580&SecMode=1&DocId=396826&Usage=2]

Παρατηρητήριο για την κοινωνία της πληροφορίας, (2007), «Μελέτη για τη χρήση τεχνολογιών πληροφορικής και επικοινωνιών στον τομέα υγείας και πρόνοιας», [WWW] Available from: http://www.observatory.gr/files/meletes/Υγεία%20-%20Π2%20Υφισταμενη %20κατάσταση%20έκδοση%205.pdf , σελ 19-45.

Aziz, A. N., (2005), «Health information systems design implementation and evaluation», [WWW] Available from: http://www.scribd.com/doc/7703327/Health-Information-System-Design-Implementation-Evaluation .

Beaumont, R., (2008), "Types of Health Information Systems (IS)", [WWW] Available from: http://www.fhi.rcsed.ac.uk/rbeaumont/virtualclassroom/chap12/s2/systems1.htm .

Cramm. http://www.cramm.com/

Development and Implementation of CDA R2 documents using CCD templates in the Homecare Service Electronic Health Record, by F.Campos, D.Luna, F.Gonzalez, Bernaldo de Quiros, Department of Health Informatics,Hospital Italiano of Buenos Aires at www.hl7elc.org/ihic2010/17.pdf

Electronic Health Record System. http://www.who.int/en/

Health Information Privacy http://www.hhs.gov/ocr/privacy/index.html

Health Level Seven International, [WWW] Available from: http://www.hl7.org/ .

IDABC EIF, ' European Interoperability Framework for Pan- European e-Government Services', 2004. Available from: http://europa.eu/index_el.htm

Matshidze, P., Hanmer, L., "Health Information Systems in the Private Health Sector" [WWW] Available from: http://www.hst.org.za/uploads/files/chap6_07.pdf .

OCTAVE, CERT http://www.cert.org/octave/

OECD. http://www.oecd.org/

Orgun, B. (2003), «Medical information systems using smart mobile agents and HL7» (EMAGS), [WWW] Available from: http://web.science.mq.edu.au/~borgun/Thesis.pdf .

Shorbaji, Al. N., (2001), «Health and Medical Informatics:Technical Paper»,[WWW] Available from: http://www.emro.who.int/his/ehealth/Medical Informatics.pdf .

The Union's founding principles http://europa.eu/geninfo/atoz/en/index_1_en.htm

Wulsin, L., Dougherty, A., (2008), « Health Information Technology-Electronic Health Records: A Primer» [WWW] Available from: http://www.library.ca.gov/crb/08/08-013.pdf .