ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Πολιτικές Ασφαλείας Συστήματος Ιατρικής Επιχειρησιακής Νοημοσύνης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Νταούλης

Επιβλέπων : Δημήτριος - Διονύσιος Κουτσούρης
Καθηγητής ΕΜΠ

Αθήνα, Νοέμβριος 2018

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Πολιτικές Ασφαλείας Συστήματος Ιατρικής Επιχειρησιακής Νοημοσύνης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Νταούλης

Επιβλέπων : Δημήτριος - Διονύσιος Κουτσούρης
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 29η Νοεμβρίου 2018

.....	.....	.....
Δ. Κουτσούρης	Γ. Ματσόπουλος	Π. Τσανάκας
Καθηγητής Ε.Μ.Π	Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ

Αθήνα, Νοέμβριος 2018

.....

Κωνσταντίνος Νταούλης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Ευχαριστίες

Η ενασχόλησή μου με τον τομέα της Βιοϊατρικής Μηχανικής αποτελεί τα τελευταία χρόνια μια επιθυμία, της οποίας η αρχή πραγματοποιήθηκε μέσω αυτής της διπλωματικής εργασίας.

Για το λόγο αυτό, θα ήθελα να ευχαριστήσω ιδιαιτέρως τους επιβλέποντες Δρ Ουρανία Πετροπούλου και τους υποψήφιους διδάκτορες Παναγιώτη Κατρακάζα και Μαριλένα Ταρούση, για τη δημιουργική τους καθοδήγηση και την εποικοδομητική κριτική, στοιχεία τα οποία μετά το πέρας των σπουδών μου θα αποτελέσουν σημαντικά εφόδια για την επαγγελματική μου σταδιοδρομία.

Θα ήθελα ακόμα να ευχαριστήσω τους φίλους και συναδέλφους μου, Ιωάννη Παπανικολόπουλο, Αντώνη Λουίζο και Αθανάσιο Νικολού για τη συμπαράσταση και τις συμβουλές που προσέφεραν σε τεχνικά και όχι μόνο θέματα κατά τη διάρκεια των σπουδών μου.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου, για τη στήριξη και τη βοήθεια τους όλα αυτά τα χρόνια, καθώς χωρίς αυτούς δεν θα μπορούσα να πραγματοποιήσω αυτό μου το στόχο.

Κωνσταντίνος Νταούλης

Νοέμβριος 2018

Περίληψη

Η παρούσα διπλωματική εργασία εστιάζεται στη σχεδίαση και την καταγραφή των μέτρων και πολιτικών ασφαλείας που απαιτούνται για την υλοποίηση ενός συστήματος ιατρικής επιχειρησιακής νοημοσύνης, ειδικά προσαρμοσμένο σε ασθενείς της νόσου του Πάρκινσον.

Το σύστημα ιατρικής επιχειρησιακής νοημοσύνης (Medical Business Intelligence-MBI) που περιγράφεται, θα χρησιμοποιεί συγχρόνους μηχανισμούς και τεχνικές για την ασφάλεια του. Με βάση τις αυξημένες απαιτήσεις ασφαλείας που πηγάζουν από την εφαρμογή στον τομέα της υγείας ολοκληρωμένων συστημάτων πληροφορικής, έχουν επιλεγεί συγκεκριμένοι μηχανισμοί (έξυπνες πύλες), πρωτόκολλα επικοινωνίας και αλγόριθμοι κρυπτογράφησης, που βεβαιώνουν την ασφαλή και ανώνυμη ανταλλαγή και επεξεργασία ιατρικών δεδομένων. Οι πολιτικές ασφαλείας του συστήματος αυτού σχεδιάστηκαν με τέτοιο τρόπο, ώστε να μπορούν βρίσκουν εφαρμογή σε παγκόσμια κλίμακα. Για αυτό το λόγο περιγράφεται επίσης η συμμόρφωσή του με διεθνείς κανόνες και πρότυπα ηθικής και δεοντολογίας.

Λέξεις-κλειδιά

Πάρκινσον, MBI, ιατρικά δεδομένα, ασφάλεια, ιδωτικότητα, ακεραιότητα, διαθεσιμότητα, ανωνυμία, έξυπνες πύλες, βάσεις δεδομένων, επικοινωνία, ηθική

Abstract

The purpose of this dissertation is to design and write down all the measures and policies needed for the implementation of a MedIcal Business Intelligence system, tailored to the needs of patients suffering from the Parkinson disease.

The Medical Business intelligence system described, will use modern mechanisms and techniques, regarding its own security. Based on the increased needs that come along with the implementation of integrated information systems in the healthcare sector, certain mechanisms (smart gateways), communication protocols and cryptographic algorithms have been chosen, ensuring that the exchange and modification of medical data is done in a safe and anonymous manner. This system's security policies have been designed in a way that can be applied in a global scale. This is the reason why its compliance with international rules and standards regarding ethics requirements is addressed as well.

Keywords

Parkinson, MBI, medical data, security, privacy, integrity, availability, anonymity, smart gateways, databases, communication, ethics

Περιεχόμενα

Ευρετήριο εικόνων

Ευρετήριο Πινάκων

Κεφάλαιο 1ο

1.1 Εισαγωγή

Ο όρος «ηλεκτρονική υγεία» (e-health), που δημιουργήθηκε στο δεύτερο μέρος του εικοστού αιώνα, μπορεί να βρεθεί ήδη σε περίπου 4.000.000 ιστοσελίδες. Στο τελευταίο μέρος του δέκατου ένατου και του πρώτου μέρους του εικοστού αιώνα, οι ιατρικές εφαρμογές επωφελούνταν γρήγορα από την πρόοδο που σημειώθηκε στον τομέα της αναλογικής τηλεφωνίας. Η τεχνολογία επέτρεψε όχι μόνο σε άτομα να καλέσουν το γιατρό, αλλά και νοσοκομεία να μεταδίδουν ηλεκτροκαρδιογραφήματα μέσω τηλεφωνικών γραμμών. Αυτές ήταν οι πρώτες μέρες της τηλειατρικής, ή της ιατρικής περίθαλψης που διενεργείται εξ αποστάσεως.

Ωστόσο, οι περιορισμοί του εύρους ζώνης και ο επακόλουθος χαμηλός ρυθμός μεταφοράς δεδομένων πάνω από τα χάλκινα καλώδια που χρησιμοποιήθηκαν στη συνέχεια, σε συνδυασμό με παρεμβολές και διάφορους τύπους θορύβου, έβαλαν φρένο στην επέκταση αυτών των αναλογικών τεχνικών. Έκτοτε, η έκρηξη της ψηφιοποίησης δεδομένων, της μηχανοργάνωσης και των ψηφιακών δικτύων που έχει ήδη ξεκινήσει από τα μέσα του εικοστού αιώνα να έχει κάνει τον τομέα της ιατρικής να κινηθεί πέρα από την τηλεϊατρική και έχει οδηγήσει σε πολλαπλές εφαρμογές ηλεκτρονικής υγείας. Τέτοιες εφαρμογές έχουν προκύψει από ακαδημαϊκά ερευνητικά εργαστήρια και έχουν γίνει ολοένα και περισσότερο μέρος της καθημερινής ζωής των ανθρώπων[1].

Η ψηφιακή τηλεϊατρική έχει περάσει τεράστια ανάπτυξη τα τελευταία 25 χρόνια και αποτελεί πλέον βασικό στοιχείο της ηλεκτρονικής υγείας. Επιτρέπει, μεταξύ άλλων, την ανταλλαγή ιατρικών και διοικητικών δεδομένων και τη μεταφορά ιατρικών εικόνων και εργαστηριακών αποτελεσμάτων. Η βελτίωση αυτών των διαδικασιών συνέπεσε με την τεχνολογική πρόοδο που παράγει ακόμη μεγαλύτερα εύρη ζώνης, μεγαλύτερη χωρητικότητα αποθήκευσης και επεξεργασίας, όλο και μικρότερα εξαρτήματα και υψηλότερα επίπεδα ασφάλειας. Αυτό συνέβη στο πλαίσιο της μείωσης του κόστους και των φιλικών προς το χρήστη λειτουργιών. Είναι πλέον λογικό να περιμένουμε ότι μέχρι το 2018 κάθε κάτοικος του πλανήτη μας θα έχει πρόσβαση σε ιατρικές πληροφορίες από οπουδήποτε και ανά πάσα στιγμή για να διατηρήσει την υγεία του ή να ζητήσει θεραπεία για την ασθένειά του.

Τροποποιώντας τη διάσημη διακήρυξη του Παγκόσμιου Οργανισμού Υγείας «Υγεία για όλους το 2000», που έγινε στην Άλμα Άτα του Καζακστάν, μπορούμε τώρα να μιλάμε για «ηλεκτρονική υγεία για όλους το 2018» ως αξιόπιστο και ρεαλιστικό στόχο, για τον οποίο είναι κοινή μας ευθύνη να φέρουμε σε πέρας.

Διαφορετικοί ορισμοί έχουν χρησιμοποιηθεί με την πάροδο του χρόνου για τον προσδιορισμό εφαρμογών που χρησιμοποιούν τεχνολογίες επικοινωνιών και πληροφορικής στην υπηρεσία της υγείας. Περί το 1970, ο όρος «ιατρική πληροφορική», που θεωρήθηκε τότε ως τελευταία λέξη της τεχνολογίας,

χρησιμοποιήθηκε για να αναφερθεί στην επεξεργασία ιατρικών δεδομένων από ηλεκτρονικούς υπολογιστές. Ωστόσο, η σημασία της «επεξεργασίας πληροφοριών» έπρεπε να αντικατασταθεί γρήγορα από την «επικοινωνία των πληροφοριών», όπως προκύπτει από την εξαιρετικά ταχεία ανάπτυξη του Διαδικτύου[2].

Οι εφαρμογές για την υγεία έγιναν τότε γνωστές ως «τηλεματική για την υγεία» ή «τηλεϊατρική» και τώρα « ηλεκτρονική υγεία». Η επιτάχυνση των ρυθμών μεταφοράς μέσω δικτύων διασυνδεδεμένων υπολογιστών (που είναι σήμερα της τάξεως των πολλών gigabytes ανά δευτερόλεπτο) έχει καταργήσει όλα τα εμπόδια στην ανταλλαγή ιατρικών δεδομένων, φυσιολογικών σημάτων και ιατρικών εικόνων μεταξύ υπολογιστών. Η τυποποίηση των πρωτοκόλλων ανταλλαγής μεταξύ ηλεκτρονικών υπολογιστών, όπως το πρωτόκολλο διαδικτύου για παράδειγμα, εκτός από τη βελτιωμένη δομή των ιατρικών δεδομένων και των κανόνων ασφάλειας δεδομένων, καθιστά όλο και περισσότερο δυνατή την κατανόηση και συνεργασία μεταξύ των επαγγελματιών υγείας σε διαφορετικές τοποθεσίες διαφορές στις γλώσσες[3].

Είναι πλέον σαφές ότι η αξία αυτών των εφαρμογών δεν έγκειται στην ίδια την τεχνολογία, ούτε στην ανταλλαγή δεδομένων, αλλά στην ικανότητα ανάπτυξης ανθρώπινων δικτύων ικανότητας και εμπειρογνωμοσύνης στον τομέα της υγείας. Εν ολίγοις, αυτός ο νέος τρόπος εργασίας - η δικτύωση όλων όσοι ασχολούνται με την επιχείρηση στον τομέα της υγείας - επεκτείνεται ταχέως χάρη στην τεχνολογική πρόοδο.

Ο κοινός παρονομαστής σε όλες αυτές τις τεχνολογίες είναι η ψηφιοποίηση δεδομένων, χωρίς την οποία τα δεδομένα δεν θα μπορούσαν να επιδέχονται επεξεργασίας και να ανταλλάσσονται με τον τρόπο που έχουμε συνηθίσει. Αυτός είναι ο λόγος για τον οποίο, αντί να προτείνεται μια σειρά λιγότερο ή περισσότερο περιοριστικών ακαδημαϊκών ορισμών για τη χρήση των τεχνολογιών πληροφορικής και υπηρεσιών που εφαρμόζουν την ηλεκτρονική υγεία στον τομέα της υγειονομικής περίθαλψης, η προσέγγιση συναίνεσης είναι να συγκεντρωθούν όλες αυτές οι εφαρμογές με τον όρο « ηλεκτρονική υγεία»[1].

Ο όρος «ηλεκτρονική» χρησιμοποιείται επίσης σε πολλές άλλες εφαρμογές, όπως η «ηλεκτρονική διακυβέρνηση» και η «ηλεκτρονική μάθηση», προκειμένου να τονιστεί η έννοια των ψηφιακών δεδομένων (σε αντίθεση με τα συμβατικά αναλογικά δεδομένα όπως ιατρικά αρχεία, εκτυπώσεις ηλεκτροκαρδιογραφήματος και φιλμ ακτινών Χ). Χωρίς ψηφιοποίηση δεν θα υπήρχε αυτόματη επεξεργασία και καμία στιγμιαία ανταλλαγή μέσω του δικτύου.

Ο όρος «υγεία» χρησιμοποιείται ευρέως και δεν αναφέρεται μόνο σε φάρμακα, ασθένεια, υγειονομική περίθαλψη ή νοσοκομεία. Το πεδίο εφαρμογής της ηλεκτρονικής υγείας είναι η υγεία γενικότερα με τις δύο κύριες πτυχές της, δηλαδή τη δημόσια υγεία, η οποία αποτελεί ευθύνη των κρατών και έχει ως στόχο την πρόληψη και αντιμετώπιση ασθενειών στους πληθυσμούς και την υγειονομική

περίθαλψη, η οποία απευθύνεται σε μεμονωμένους ασθενείς και θεραπεία ασθενειών[4].

Η έννοια της ηλεκτρονικής υγείας καλύπτει έτσι όλες τις πτυχές της υγείας, όχι μόνο την υγειονομική περίθαλψη. Ο όρος εξελίσσεται σταδιακά και αναφέρεται στη σκελετική δομή για όλες τις λειτουργίες των συστημάτων υγείας. Δεν πρόκειται απλώς για τη βελτίωση του συνόλου των επιδημιολογικών δεδομένων ή για την ανταλλαγή φακέλων μεταξύ των ιδρυμάτων δημόσιας υγείας, αλλά σχετίζεται όλο και περισσότερο με τη χρήση τεχνολογιών ηλεκτρονικής υγείας για την πραγματοποίηση των αναγκαίων μεταρρυθμίσεων στα συστήματα υγείας και, ως εκ τούτου, για τη γενικότερη βελτίωση της υγείας σε παγκόσμια κλίμακα. Τα παραδείγματα κυμαίνονται από μεμονωμένα μέτρα προώθησης της υγείας στο πλαίσιο του σπιτιού, του χώρου εργασίας ή του σχολείου μέχρι την εξατομικευμένη παροχή υγειονομικής περίθαλψης σε μεμονωμένους ασθενείς σε πολλά περιβάλλοντα. Ένα από τα λάθη που γίνονται συχνά εξαρχής είναι να περιγραφούν οι εξελίξεις στον τομέα της ηλεκτρονικής υγείας αποκλειστικά στον τομέα της υγειονομικής περίθαλψης, καθώς οι εξελίξεις θεωρούνται πιο θεαματικές και άμεσα επωφελείς[5].

Η ηλεκτρονική υγεία είναι ίσως το μεγαλύτερο κύμα αλλαγών στην υγειονομική περίθαλψη από το κύμα της νέας δημόσιας διοίκησης μεταξύ του 1980 και του 2000. Η ανάπτυξη της ηλεκτρονικής υγείας μπορεί να θεωρηθεί ως μια μεταβολή του διακυβεύματος με στόχο την παροχή στους ασθενείς αυξημένης πρόσβασης και επιρροής όσον αφορά την κατάστασης της υγείας τους, δίνοντας έμφαση σε όρους όπως «εξουσιοδότηση» , «διαφάνεια ασθενούς» και «χειραφέτηση ασθενούς».

Πολλοί βασικοί συντελεστές βλέπουν μάλιστα την ηλεκτρονική υγεία ως πανάκεια για την επικείμενη έλλειψη πόρων για την υγειονομική περίθαλψη. Ωστόσο, καθώς αναπτύσσονται και νέες τεχνικές και συστήματα ηλεκτρονικής υγείας, τόσο στο δημόσιο όσο και στην ιδιωτική αγορά, προκύπτουν νέοι τομείς ανησυχίας και εμπόδια, πολλά από τα οποία δεν προβλέπονταν από τους ίδιους τους προγραμματιστές. Πρέπει να αντιμετωπιστούν πτυχές όπως οι νόμοι και οι κανονισμοί, τα ψηφιακά χάσματα, η εμπιστοσύνη, η ισότητα και τα θέματα ευπάθειας, η αλλαγή της διανομής ενέργειας, η ακεραιότητα και η ασφάλεια των ασθενών, η τεχνολογική ασφάλεια, η ηθική και το εργασιακό περιβάλλον των επαγγελματιών υγείας, ώστε να υπάρξει μια γενική κατανόηση της ηλεκτρονικής υγείας.

Τα παραπάνω δείχνουν ότι η ηλεκτρονική υγεία είναι μια πραγματικά πολύπλευρη περιοχή που απαιτεί διεπιστημονικές προοπτικές και συζητήσεις που πρέπει να καταστούν κατανοητές[6][7].

1.2 Στόχος και αντικείμενο της διπλωματικής εργασίας

Η παρούσα διπλωματική εργασία παρουσιάζει μια σύντομη βιβλιογραφική αναφορά στην ηλεκτρονική υγεία και τα ζητήματα ασφαλείας που προκύπτουν σε αυτή και

εστιάζει στην ανάλυση, το σχεδιασμό και την ανάπτυξη των πολιτικών ασφαλείας που χρησιμοποιούνται σε ένα σύστημα ιατρικής επιχειρησιακής νοημοσύνης.

Ο στόχος του αντικειμένου που παρουσιάζεται, είναι η υποβοήθηση στον εκάστοτε ασθενή, ώστε να ενθαρρυνθεί η χρήση του συστήματος από αυτόν, αλλά και να νιώσει πιο ασφαλής, όσον αφορά τα προσωπικά δεδομένα που παραδίδει στο σύστημα, μέσα από την καταγραφή των πολιτικών ασφαλείας του.

Ως πολιτική ασφαλείας ορίζεται το τι χρειάζεται ένα σύστημα, ένα οργανισμός η μία οντότητα για να είναι ασφαλής. Για τα συστήματα, οι πολιτικές ασφαλείας ασχολούνται με τους περιορισμούς στις λειτουργίες και τη ροή μεταξύ τους, τους περιορισμούς στην πρόσβαση από εξωτερικά συστήματα, την προστασία από κακόβουλες ενέργειες συμπεριλαμβανομένων των προγραμμάτων και την πρόσβαση στα δεδομένα από τους ανθρώπους.

Οι πολιτικές ασφαλείας που περιγράφονται κι αναπτύσσονται επιχειρούν να συμβάλλουν στη δημιουργία ενός συστήματος ιατρικής επιχειρησιακής νοημοσύνης που θα ακολουθεί όσο το δυνατόν πιστότερα ορισμένους κανόνες ασφαλείας υπό συγκεκριμένους περιορισμούς.

Η εφαρμογή των πολιτικών ασφαλείας αυτών έγινε για σύστημα που αφορά τη νόσο του Πάρκινσον, αλλά μπορεί να εφαρμοστεί και σε πληθώρα άλλων αντίστοιχων συστημάτων.

Από την ανάλυση που έγινε στο εισαγωγικό τμήμα του κεφαλαίου αυτού, γίνεται αντιληπτό ότι εξαιτίας της πολυπλοκότητας των σύγχρονων συστημάτων για την ηλεκτρονική υγεία, υφίσταται η ανάγκη για ολοκληρωμένες λύσεις στον τομέα της ασφάλειας τους, οι οποίες θα ανταποκρίνονται στην πολυδιάστατη φύση του προβλήματος αυτού.

Ένεκα των παραπάνω, οι πολιτικές ασφαλείας που αναπτύχθηκαν για το παρόν σύστημα προσφέρει οφέλη σε όποιον επιθυμεί να συμμετάσχει στο σύστημα. Αρχικά, επιτρέπει στους μη ιδιαιτέρως έμπειρους χρήστες των τεχνολογιών πληροφορικής και υπηρεσιών να μπορούν να συνθέσουν τους δικούς τους κανόνες ασφαλείας μέσα στο σύστημα, οι οποίοι θα ανταποκρίνονται στις δικές τους ανάγκες, χωρίς να είναι αναγκαίο να λάβουν προηγουμένως κάποια ιδιαίτερη εξειδίκευση για το λόγο αυτό. Επιπλέον, οι εφαρμοζόμενοι κανόνες και πρότυπα για την ασφάλεια του συστήματος ιατρικής επιχειρησιακής νοημοσύνης προσφέρουν τη δυνατότητα προσαρμογής σε παρούσες ανάγκες και τυχόν ιδιαίτερες ανάγκες ενός συμμετέχοντα σε αυτό.

1.3 Δομή της Διπλωματικής εργασίας

Η παρούσα διπλωματική εργασία είναι δομημένη σε έξι κεφάλαια, καθένα από τα οποία συμβάλλει με σαφή τρόπο στην αποτελεσματική παρουσίαση του θέματος των πολιτικών ασφαλείας σε ένα σύστημα ιατρικής επιχειρησιακής νοημοσύνης. καθώς επίσης και στην ανάδειξη των μηχανισμών και τεχνικών που αναπτύχθηκαν και

εφαρμόστηκαν σε αυτό. Στη συνέχεια παρατίθεται συνοπτικά η διάρθρωση των κεφαλαίων της παρούσας διπλωματικής.

Κεφάλαιο 1ο

Παρουσιάζει το πλαίσιο το οποίο θα εξετάσει η εργασία, όπως επίσης το αντικείμενο τους στόχους και τη συμβολή της.

Κεφάλαιο 2ο

Πραγματοποιεί μια ανάλυση των συμμετεχόντων στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης. Πιο συγκεκριμένα, παρουσιάζει τους ενδιαφερόμενους και καταγράφει τις απαιτήσεις τους από ένα τέτοιο σύστημα, αλλά και τις αρμοδιότητες που έχουν σε αυτό.

Κεφάλαιο 3ο

Παραθέτει μια σύντομη επισκόπηση του συστήματος ιατρικής επιχειρησιακής νοημοσύνης, δίνοντας έμφαση στις υπηρεσίες που παρέχει αλλά και τις λειτουργίες του.

Κεφάλαιο 4ο

Καταγράφει τις ανάγκες ασφαλείας στα πληροφοριακά συστήματα εν γένει και εστιάζει στις ηλεκτρονικές υπηρεσίες υγείας. Στη συνέχεια, παρουσιάζει στο απαιτούμενο βάθος τους μηχανισμούς και τις τεχνικές για την ασφάλεια που χρησιμοποιήθηκαν κατά τη σχεδίαση του συστήματος, με βάση τις ανάγκες που προέκυψαν.

Κεφάλαιο 5ο

Παρουσιάζει εν συντομία το πρότυπο ηθικής κι δεοντολογίας με βάση το οποίο σχεδιάστηκε το σύστημα ιατρικής επιχειρησιακής νοημοσύνης. Στη συνέχεια παραθέτει τους ελέγχους και τις διοικητικές παραμέτρους που διασφαλίζουν την ομαλή λειτουργία του, αλλά και το πώς εναρμονίζεται το σύστημα σε σχέση με το πρότυπο.

Κεφάλαιο 6ο

Παρουσιάζει μια σύνοψη της ασφάλειας του συστήματος και τα εξαγόμενα συμπεράσματα

Κεφάλαιο 2ο

Ενδιαφερόμενοι και συμμετέχοντες στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης

Όπως και σε κάθε άλλο διαδραστικό σύστημα (στην υγεία και όχι μόνο), το πρώτο που πρέπει να καθοριστεί είναι το προφίλ των συμμετεχόντων και ο αντίστοιχος ρόλος που παίζουν στην αποτελεσματική λειτουργία του συστήματος. Στην περίπτωση του συστήματος επιχειρησιακής νοημοσύνης για την παρακολούθηση ασθενών με Πάρκινσον, κατηγοριοποιούμε τους συμμετέχοντες στα εξής κατηγορίες, καθεμιά από τις οποίες αντιπροσωπεύει διαφορετικό τύπου χρήστη και έχει διαφορετικές απαιτήσεις ή και αρμοδιότητες.

2.1 Παρκινσονικοί Ασθενείς

Οι ασθενείς που πάσχουν από τη νόσο του Πάρκινσον ανήκουν σε μια ομάδα ασθενών που παρουσιάζουν διαταραχές του νευρικού τους συστήματος, οι οποίες έρχονται ως αποτέλεσμα της σταδιακής απώλειας των κυττάρων του εγκεφάλου που είναι υπεύθυνα για την παράγωγη ντοπαμίνης.

Τα τέσσερα πιο βασικά συμπτώματα της ασθένειας του Πάρκινσον είναι :

- Τρέμουλο στα χέρια, στις παλάμες, στα πόδια, στο πρόσωπο και στο σαγόνι
- Δυσκαμψία ή και ακαμψία στα άκρα και στον κορμό
- Βραδυκινησία, δηλαδή μειωμένη κινητικότητα ή βραδύτητα στις καθημερινές κινήσεις
- Αστάθεια, ή διαταραχή της ισορροπίας και του συγχρονισμού

Όσο τα συμπτώματα αυτά εντείνονται, οι ασθενείς μπορεί να παρουσιάσουν δυσκολίες στην ομιλία, στο περπάτημα, ή σε άλλες ανάγκες τους.

Η νόσος του Πάρκινσον συνήθως επηρεάζει ανθρώπους από την ηλικία των 60 και πάνω. Τα πρώτα συμπτώματα της ασθένειας είναι ανεπαίσθητα και στη συνέχεια εμφανίζονται σταδιακά, ενώ σε μερικούς ανθρώπους η ασθένεια εξελίσσεται πιο γρήγορα από άλλους. Όσο προχωράει η ασθένεια, το τρέμουλο και η αστάθεια, τα οποία εμφανίζονται στην πλειονότητα των ανθρώπων που πάσχουν από αυτήν, μπορεί να εμποδίζουν την ολοκλήρωση των καθημερινών τους δραστηριοτήτων. Αυτό μπορεί να οδηγήσει σε συναισθηματικές αλλαγές στη ζωή του ασθενούς, ακόμα και σε κατάθλιψη, αλλά και σε δυσκολίες στην ομιλία, στην κατάποση, στην ούρηση και στον ύπνο[8] [9].

2.1.1 Απαιτήσεις των ασθενών

Οι ασθενείς γενικά είναι θετικά προδιαθετημένοι απέναντι στις υπηρεσίες υγείας που βασίζονται στην σωματική άσκηση, ενώ συμφωνούν ότι μπορεί να συμβάλλει

στην πρόληψη τυχόν πτώσεων που ενδεχομένως να προκαλέσει η αστάθεια, στη βελτίωση της υγείας και της ποιότητας ζωής τους. Επιπλέον, βλέπουν θετικά την διαμόρφωση της άσκησης ως παιχνίδι, καθώς θεωρούν ότι είναι πολύ πιο ενδιαφέρουσα κάποια άσκηση, αν απαιτεί κάποια πνευματική διεργασία ταυτόχρονα. Το ενδιαφέρον των ασθενών για τεχνολογίες που τους επιτρέπει να εκτελούν αυτού του είδους τις ασκήσεις από το σπίτι, είναι αρκετά μεγάλο, καθώς πολλές φορές η σωματική τους κατάσταση, ή ακόμα και οι καιρικές συνθήκες δεν τους επιτρέπουν μεγάλες μετακινήσεις. Ωστόσο, προηγούμενη γνώση έχει δείξει ότι οι νοσούντες από Πάρκινσον έχουν, κυρίως επειδή πρόκειται για άτομα μεγάλης ηλικίας, περιορισμένες έως καθόλου γνώσεις πάνω σε τεχνολογίες πληροφορικής και τηλεπικοινωνιών, οπότε η διαμόρφωση των παιχνιδιών θα πρέπει να είναι αποκλειστική ευθύνη των ειδικών, του διαχειριστή κλπ.

Λόγω του γεγονότος ότι σε χώρες όπως η Ελλάδα οι γνώσεις των μεγαλύτερων σε ηλικία ανθρώπων πάνω σε τέτοιες τεχνολογίες είναι περιορισμένη, οι ασθενείς θα πρέπει να λαμβάνουν επαρκή εκπαίδευση ώστε να μπορούν να έρχονται σε διεπαφή με τις υπηρεσίες του συστήματος ιατρικής επιχειρησιακής νοημοσύνης, αλλά και να εκπαιδεύονται παράλληλα με κάποιο από τα άτομα που τους φροντίζει. Χρειάζονται να αποκτήσουν μια αρχική εξοικείωση με τέτοιου είδους τεχνολογίες, ώστε να αντιλαμβάνονται καλύτερα τις υπηρεσίες του συστήματος, ή τουλάχιστον το πρόγραμμα εξάσκησης να είναι προσαρμοσμένο στις ελλιπείς τους γνώσεις πάνω στις τεχνολογίες αυτές[8].

Έχει δειχθεί ότι οι ασθενείς εγείρουν συγκεκριμένες απαιτήσεις όσον αφορά τη χρηστικότητα της διεπαφής τους με το σύστημα. Τέτοιες απαιτήσεις είναι :

- Το μέγεθος των πλήκτρων, το οποίο θα πρέπει να διευκολύνει τη χρήση τους από τους ασθενείς
- Η απόσταση των πλήκτρων μεταξύ τους
- Η ένταση της ομιλίας και του ήχου γενικότερα
- Η πολυπλοκότητα των λειτουργιών που καλείται να εκτελεί

Είναι σημαντικό για τους ασθενείς να βρουν μια αποδοτική οικονομικά λύση. Αυτό σημαίνει ότι θα ήταν χρήσιμο για αυτούς που είναι απομονωμένοι να ενσωματωθεί στην πλατφόρμα του συστήματος MBI ένα δωρεάν μέσο επικοινωνίας με άλλους χρήστες, κοντινούς συγγενείς ή και τους θεράποντες τους, στο οποίο να μπορούν να συζητήσουν την πρόοδο τους. Ένα τέτοιο μέσο θα μπορούσε να είναι λόγου χάρη το Skype.

Πρέπει επίσης να δοθεί βάση στο γεγονός πως η εγκατάσταση οπτικών συστημάτων στο χώρο όπου θα λαμβάνουν χώρα οι ασκήσεις δεν θα εγείρουν ανησυχίες για την ιδιωτικότητα του ασθενούς. Αντίθετα, τέτοιου είδους ανησυχίες δε φαίνεται να υπάρχουν για τους αισθητήρες βάθους που χρησιμοποιούνται[10].

Οι ασθενείς φαίνεται να προτιμούν την οθόνη της τηλεόρασης τους για την οπτικοποίηση της άσκησης τους, σε σχέση με την οθόνη ενός υπολογιστή ή μιας άλλης έξυπνης συσκευής (όπως για παράδειγμα ένα tablet). Επιθυμούν επίσης να

έχουν ηχητικές και οπτικές ενδείξεις για την έναρξη της συνεδρίας και το διάστημα κατά το οποίο η κάμερα είναι ανοιχτή και τους καταγράφει. Ταυτόχρονα, δηλώνουν άνετοι με τη χρήση του Skype, ως μέσο για να λαμβάνουν αξιολόγηση της προόδου τους, από τον ειδικό, όταν αυτός βρίσκεται σε διαφορετικό χώρο. Τέλος, επιθυμούν την αξιολόγηση της επίδοσης τους κατά τη διάρκεια του παιχνιδιού, σε πραγματικό χρόνο από ψηφιακά μέσα, μέσω οπτικής τεχνολογίας η τεχνολογίας διεπαφής, ώστε να μπορούν άμεσα να βελτιώσουν την απόδοση τους[11].

2.2 Επαγγελματίες υγείας

Ο Παγκόσμιος Οργανισμός υγείας ορίζει τους επαγγελματίες υγείας ως αυτούς που φροντίζουν για την υγεία του ασθενούς διαμέσου της εφαρμογής αρχών και διαδικασιών θεραπείας και φαρμακευτικής αγωγής που έχουν βασιστεί σε αποδείξεις. Είναι αυτοί που μελετούν, διαγιγνώσκουν, θεραπεύουν και προλαμβάνουν ανθρώπινες ασθένειες, τραυματισμούς και άλλες σωματικές ή ψυχικές δυσλειτουργίες, με γνώμονα τις ανάγκες του πληθυσμού που υπηρετούν. Συμβουλεύουν ή και εφαρμόζουν προληπτικά και θεραπευτικά μέτρα και προωθούν την υγεία με απώτερο σκοπό να ικανοποιήσουν τις ατομικές και συνολικές ανάγκες και προσδοκίες περίθαλψης του πληθυσμού, αλλά και να βελτιώσουν την ποιότητα της. Επίσης, διεξάγουν έρευνα και βελτιώνουν ή αναπτύσσουν θεωρίες, μεθόδους και τεχνικές για να προχωρήσουν την φροντίδα βασισμένη σε αποδείξεις. Τα καθήκοντα τους μπορεί επιπλέον να περιλαμβάνουν και την επίβλεψη άλλων ανθρώπων που εργάζονται στο χώρο της υγείας[12].

Όσον αφορά τη νόσο του Πάρκινσον, οι επαγγελματίες υγείας αποτελούνται από γιατρούς (γενικούς και εξειδικευμένους), επαγγελματίες νοσηλευτές και τους φαρμακοποιούς.

2.2.1 Απαιτήσεις των επαγγελματιών υγείας

Η ολιστική υποδομή του συστήματος επιχειρησιακής νοημοσύνης που έχει εφαρμοστεί στη ρύθμιση του σπιτιού του ασθενούς όσο και το ιατρικό κέντρο έχει σκοπό να:

- Παρέχει τεχνολογία η οποία είναι χαμηλού κόστους, απλή στην εγκατάσταση και στο χειρισμό (αφορά και τους επαγγελματίες υγείας εκτός από τους ασθενείς).
- Παρέχει οπτικοποιημένη βοήθεια στους ασθενείς στην οθόνη τους κατά τη διάρκεια του «παιχνιδιού», ώστε να μπορούν να βελτιώσουν τον τρόπο εκτέλεσης των ασκήσεων.
- Παρέχει εργαλεία για την εκτίμηση του κινδύνου πτώσης ενός ασθενούς τα οποία επικεντρώνονται κυρίως στους εγγενείς παράγοντες που σχετίζονται με την πιθανότητα πτώσης και ταξινόμηση του ανάλογα με αυτήν σε μια από τις ακόλουθες κατηγορίες:
    i. μηδενικής επικινδυνότητας

ii. χαμηλής επικινδυνότητας
iii. υψηλής επικινδυνότητας

- Παρέχει εργαλεία τα οποία βοηθούν τη σχεδίαση υψηλού επιπέδου «παιχνιδιών» (παιχνίδια εικονικής πραγματικότητας), τα οποία θα προστατεύουν τους ασθενείς από πτώσεις διαμέσου φιλικής για το χρήστη-ασθενή άσκησης, ανάλογα με το επίπεδο κινδύνου για ένα τέτοιο ατύχημα και ακολουθώντας μια δια βίου προοπτική.
- Παρακολουθεί σε βάθος χρόνου τη φυσική κατάσταση του ασθενούς αναλύοντας την απόδοσή του κατά τη διάρκεια των ασκήσεων αξιολόγησης και αποκατάστασης της κίνησης του.
- Αναδιαμορφώνει το πρόγραμμα πρόληψης προσαρμόζοντας το συνεχώς, ώστε να αποτελεί την καλύτερη δυνατή λύση που αρμόζει στον ασθενή παίρνοντας ως δεδομένο τα επικαιροποιημένα στοιχεία από τις επιδόσεις του χρήστη.
- Παρακινεί όλους τους συμμετέχοντες του συστήματος μέσω e-learning (μάθηση εξ αποστάσεως)[13][10].

2.3 Ανεπίσημοι φροντιστές

Ένας ανεπίσημος φροντιστής είναι ένα άτομο, όπως ένα μέλος της οικογένειας, ένας φίλος ή ένας γείτονας, ο οποίος παρέχει τακτική και συνεχή φροντίδα και βοήθεια στο άτομο που χρειάζεται υποστήριξη. Η χρήση του επίθετου «ανεπίσημος» δεν σημαίνει ότι η παρεχόμενη περίθαλψη θεωρείται ότι είναι περιστασιακή ή στερείται δομής και συγκεκριμένης διαδικασίας. Πρόκειται μάλλον για τη διάκριση της μη αμειβόμενης φροντίδας από την οικογένεια, τους φίλους ή τους γείτονές του σε σχέση με αυτή που παρέχεται από επίσημους οργανισμούς ή ιδρύματα, η οποία παρέχεται μετά από συνδρομή που καταβάλλει ο δικαιούχος (ενδεχομένως περιλαμβάνει και κάποια κρατική επιδότηση), ή παρέχεται από (απαραιτήτως) εκπαιδευμένους επαγγελματίες[14].

Οι ανεπίσημοι φροντιστές διαδραματίζουν σημαντικό ρόλο στη ζωή πολλών ανθρώπων. Το είδος της φροντίδας που παρέχουν ποικίλλει, από την προσωπική φροντίδα μέχρι τη μεταφορά σε εξειδικευμένο κέντρο ιατρικής περίθαλψης. Μπορούν να παρέχουν φροντίδα σε συνδυασμό με τις επίσημες δομές περίθαλψης, να μοιράζονται τη φροντίδα του ασθενούς με άλλους ανεπίσημους φροντιστές ή να είναι οι μοναδικοί φροντιστές. Ο υπεύθυνος για την πλειοψηφία της άτυπης φροντίδας είναι γνωστός ως ο πρωταρχικός φροντιστής.

Η φροντίδα που προσφέρεται από αυτούς προς τους ασθενείς είναι μια έκφραση της σχέσης τους σε μια ώρα ανάγκης, ακόμα κι αν αυτό δεν είναι πάντα η πρώτη επιλογή του φροντιστή. Ενώ η φροντίδα μπορεί να είναι μια ηθική ανταμοιβή για αυτούς, οι φροντιστές μπορεί επίσης να βιώσουν το άγχος της κοινωνικής απομόνωσης, της σωματικής και συναισθηματικής καταπόνησης, και τις μειωμένες ευκαιρίες εκπαίδευσης και απασχόλησης[15][13].

2.4 Διαχειριστής του συστήματος ιατρικής επιχειρησιακής νοημοσύνης

Ο διαχειριστής είναι υπεύθυνος για το σχεδιασμό και την καθημερινή συντήρηση της πλατφόρμας του συστήματος επιχειρησιακής νοημοσύνης στο Σύννεφο (Cloud) καις στο Διαδίκτυο (Internet). Αυτό περιλαμβάνει το σχεδιασμό, την υλοποίηση και την εξυπηρέτηση όλων των φορέων που χρησιμοποιούν πλατφόρμες που παρέχουν αυτές τις υπηρεσίες. Οι αρμοδιότητες του διαχειριστή δεν περιορίζονται μόνο στα παραπάνω, αλλά εκτείνονται πέρα από αυτές, όπως φαίνεται και στη συνέχεια[16][17].

2.4.1 Ευθύνες και αρμοδιότητες του διαχειριστή του συστήματος

Οι ευθύνες του διαχειριστή περιλαμβάνουν, αλλά δεν περιορίζονται στα παρακάτω:

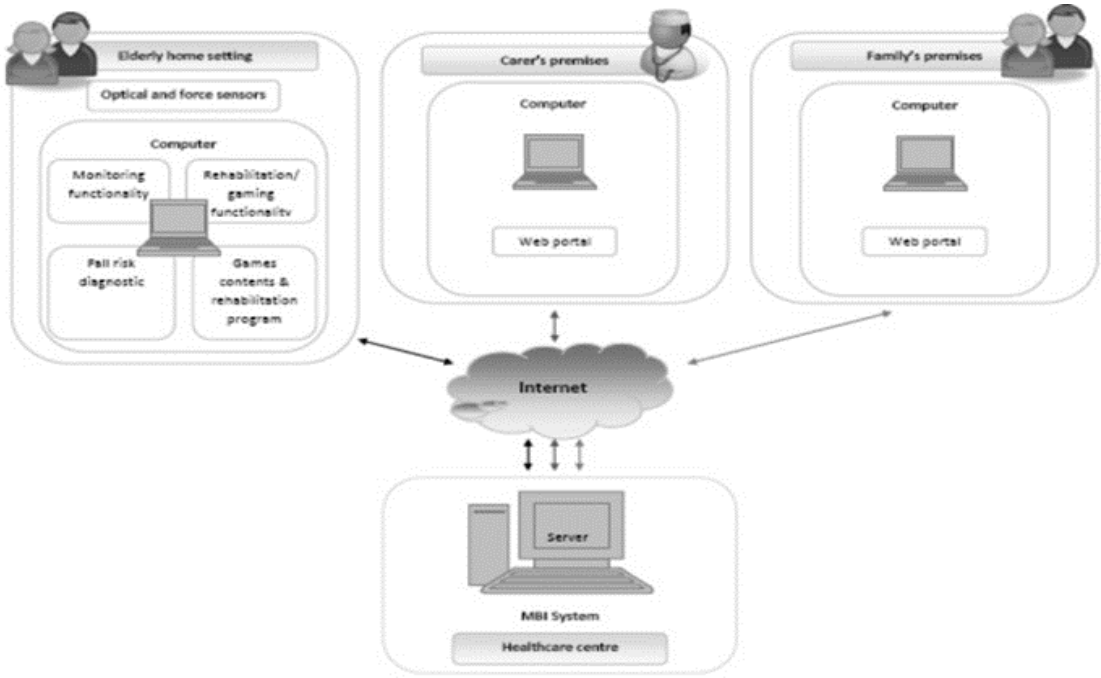
- Την υποστήριξη της λειτουργίας των δικτύων και την παροχή τεχνικής υποστήριξης με την επίλυση των ζητημάτων διακοπής λειτουργίας στη σχέση πελατών-δικτύων που σχετίζονται με την παροχή υπηρεσιών και των ζητημάτων που περιλαμβάνουν προβλήματα που αφορούν το δίκτυο γενικότερα.
- Σχεδίαση νέων προσφορών προϊόντων που σχετίζονται με τις υπηρεσίες του συστήματος.
- Τον εντοπισμό παρουσιαζόμενων προβλημάτων στις υπηρεσίες του συστήματος και επίλυση τους μέσα στην ομάδα.
- Τη δημιουργία αυτοματισμών σε όλα τα σημεία των καθημερινών εργασιών και υποχρεώσεων.
- Την ολοκλήρωση αιτημάτων εργασίας από τις διάφορες ομάδες υπηρεσιών.
- Τη δημιουργία αναφορών και αναλύσεων για τις τάσεις και την απόδοση μέσα στο δίκτυο παροχής υπηρεσιών.
- Να ενημερώνει τα μέρη του συστήματος για όλα τα ζητήματα ασφαλείας, ακεραιότητας του δικτύου και άλλα θέματα κατάχρησης που φορούν το σύνολό του ή και μέρος αυτού.
- Να παρέχει υπηρεσίες κατόπιν εντολής ή απαίτησης (on call) και να είναι διαθέσιμος εκτός ωραρίου για προβλήματα που αφορούν το server.
- Να εργάζεται σε πληθώρα εργασιών συντήρησης και βελτιστοποίησης.
- Να εκτελεί και να ολοκληρώνει καθήκοντα που σχετίζονται με το σύστημα MBI, όπως κατασκευή νέων υποδομών, αλλαγές στην υπάρχουσα υποδομή και μετακίνηση υπηρεσιών και εξοπλισμού σε καλύτερά μέρη.
- Να διευκολύνει τη βέλτιστη λειτουργία του διακομιστή[17][16].

Κεφάλαιο 3ο

Υπηρεσίες και λειτουργίες του συστήματος ιατρικής επιχειρησιακής νοημοσύνης για την ασθένεια του Πάρκινσον

Οι στόχοι του συστήματος ιατρικής επιχειρησιακής νοημοσύνης που απευθύνεται σε άτομα που πάσχουν από τη νόσο του Πάρκινσον είναι η ενσωμάτωση, η ανάπτυξη κατάλληλης υποδομής και η εφαρμογή πιλοτικών μελετών για την εφαρμογή μιας ολοκληρωμένης και ολιστικής υπηρεσίας διαχείρισης και φροντίδας του ασθενούς μέσω χρήσης καινοτόμων τεχνολογιών. Για αυτό το λόγο θα βασίζεται σε τεχνολογίες πληροφορικής, διαδικτύου και εικονικής πραγματικότητας, όπου μέσω της εκμετάλλευσης τους θα απευθύνεται στους ασθενείς τόσο με προληπτικό τρόπο (για παράδειγμα εκπαιδεύοντας τους για να προστατεύονται από τυχόν πτώσεις, βελτιώνοντας δηλαδή την ευστάθεια τους), όσο και αντιδρώντας στις μετρήσεις τους (ανιχνεύοντας τα επίπεδα ασφαλείας τους και υποστηρίζοντας τους σε ένα ανεξάρτητο τρόπο ζωής). Υπόσχεται δηλαδή να επαναπροσδιορίσει την θεραπεία των ασθενών, παρακινώντας τους να ασκούνται περισσότερο με φιλικό προς το χρήστη τρόπο.

Οι κύριες προβλεπόμενες ιδιότητες του MBI θα είναι η προσιτή του φύση τόσο από άποψη κόστους όσο και ανθρώπινων παραγόντων, καθώς και η ακρίβειά του για την αξιολόγηση των δεικτών του επιπέδου κινδύνου τόσο για τη διάγνωση όσο και για τον προσανατολισμό της στρατηγικής αποκατάστασης και εκπαίδευσης. Το προαναφερθέν σύστημα επιχειρησιακής νοημοσύνης είναι λοιπόν ένα μοντέλο συνεργασίας και τα υποσυστήματα του απεικονίζονται συνοπτικά στο παρακάτω σχήμα.



Εικόνα 1: Η δομή του συστήματος MBI

3.1 Υπηρεσίες του συστήματος ιατρικής επιχειρησιακής νοημοσύνης

Οι υπηρεσίες που πρέπει να παρέχει η πλατφόρμα για την ικανοποίηση των απαιτήσεων του Ασθενούς και των επαγγελματιών υγείας παρατίθενται παρακάτω:

- Παρέχει εργαλεία για τη διαχείριση των ιατρικών αρχείων του ασθενούς.
- Παρέχει εργαλεία συστήματος λήψης αποφάσεων για την ανάλυση της κίνησης και την αξιολόγηση του κινδύνου πτώσης με βάση την κινηματική ανάλυση των ασκήσεων που εκτελούνται από τους ασθενείς.
- Παρέχει διαδικτυακή πύλη που παρέχει εργαλεία λογισμικού και διεπαφή χρήστη για σχεδιασμό σχεδίου αποκατάστασης.
- Δημιουργεί ειδοποιήσεις με γνώμονα το περιβάλλον, δηλαδή το σύστημα MBI μέσω των «σοβαρών παιχνιδιών» (serious games) προσφέρει υπηρεσίες για την πραγματική παρακολούθηση του καρδιακού ρυθμού, της θερμοκρασίας και της υγρασίας στο χώρο του ασθενούς.
- Είναι μια πλατφόρμα εκτέλεσης παιχνιδιών με χαμηλό κόστος, εύκολη εγκατάσταση στο σπίτι του ασθενούς και εύκολη λειτουργία.
- Παρέχει εφαρμογή Web-portal για απομακρυσμένη διαμόρφωση του παιχνιδιού.
- Παρέχει εφαρμογή βιντεοκλήσης και ηλεκτρονικό ταχυδρομείο, το οποίο επιτρέπει στους ασθενείς να επικοινωνούν με ιατρικούς εμπειρογνώμονες με φωνή χρησιμοποιώντας μικρόφωνο, βίντεο χρησιμοποιώντας μια κάμερα web και άμεση ανταλλαγή μηνυμάτων μέσω Internet.
- Παρέχει εφαρμογή για ηλεκτρονική μάθηση.

3.2 Λειτουργίες του συστήματος ιατρικής επιχειρησιακής νοημοσύνης

Οι λειτουργίες υψηλού επιπέδου λοιπόν του συγκεκριμένου μοντέλου συνεργασίας περιγράφονται παρακάτω και είναι οι εξής:

Η λειτουργία παρακολούθησης από απόσταση (tele-monitoring): Οι ισχυρές, αλλά ταυτόχρονα μη ενοχλητικές συσκευές παρακολούθησης που βασίζονται σε οικονομικά αποδοτικές τεχνολογίες για την αξιολόγηση κινήσεων, θα καταγράφουν και θα μεταφέρουν δεδομένα στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης. Ο υπολογιστής που είναι εγκατεστημένος στους χώρους των ασθενών θα συλλέγει αυτόματα τα δεδομένα που συλλαμβάνονται από τις συσκευές, θα τα επεξεργάζεται και θα τα αποστέλλει μετά τον τερματισμό κάθε συνεδρίας με ασφαλή τρόπο στον κεντρικό αποθηκευτικό του συστήματος MBI[18].

Οι λειτουργίες παιγνίων και αποκατάστασης (Gaming and Rehabilitation): Διαμέσου του κατάλληλου υλικού (πληκτρολόγιο και ποντίκι, οθόνη αφής ή ακόμα κι

τηλεχειριστήριο), που διασφαλίζει την επικοινωνία του ανθρώπου με το λογισμικό, οι ασθενείς θα έχουν της παρακάτω δυνατότητες:

i. Να συνδέονται και να αποσυνδέονται (login/logout), να έχουν πρόσβαση στο μενού και στα προσωπικά, ειδικά σχεδιασμένα για αυτούς προγράμματα εκπαίδευσης και αποκατάστασης πού αφορούν την κινητικότητα, τη δύναμη, την ισορροπία και την αντοχή τους, ανάλογα με τις δυνατότητες τους.

ii. Να δέχονται αυτόματα και σε πραγματικό χρόνο οδηγίες, κατευθύνσεις και επιτήρηση από το σύστημα, χωρίς την παρέμβαση εξωτερικού συνεργάτη. Η δυνατότητα παρακολούθησης από απόσταση των ασθενών σε αυτό το σημείο επιτρέπει την αξιολόγηση των ασθενών σε πραγματικό χρόνο, κατά τη διάρκεια του παιχνιδιού, μέσω των ρυθμίσεων των ανιχνευτών που παρέχονται από τις ρυθμίσεις ελέγχου του παιχνιδιού[19].

iii. Να μπορούν να δέχονται και να δίνουν σχόλια μέσω μηνυμάτων στην εφαρμογή δικτύου (Web portal), η οποία θα αναλυθεί παρακάτω[20].

Η λειτουργία της αυτοματοποιημένης υποστήριξης αποφάσεων υγείας: Τα δεδομένα που αποθηκεύονται στο κεντρικό αποθηκευτικό χώρο θα επιτρέψουν την εκτίμηση των λειτουργικών χαρακτηριστικών των ασθενών (π.χ. εξέλιξη της δομής σκελετικής άρθρωσης που ορίζεται με χωροχρονικές παραμέτρους, εύρη κινήσεων, γωνίες άρθρωσης, επίπεδο τρόμου κτλ.). Με βάση αυτά τα λειτουργικά χαρακτηριστικά σε πραγματικό χρόνο και χάρη σε μια διαδικασία μηχανικής μάθησης, το σύστημα ιατρικής επιχειρησιακής νοημοσύνης θα διακρίνει, από τη μία συνεδρία παρακολούθησης μέχρι την επόμενη, τα συμπωματικά λειτουργικά χαρακτηριστικά από τα μη συμπωματικά και θα τα ταξινομεί σε επίπεδα κινδύνου. Όλες αυτές οι σχετικές πληροφορίες θα εμφανίζονται στο χρήστη μέσω γραφικού περιβάλλοντος (GUI). Οι διαθέσιμες πληροφορίες θα βοηθήσουν τους φροντιστές να παρακολουθήσουν αποτελεσματικά την κατάσταση κινητικότητας του ατόμου με την πάροδο του χρόνου, να εντοπίσουν τα προβλήματα και τους σχετικούς κινδύνους και να αποφασίσουν αν χρειάζεται να εφαρμοστούν ενεργητικές ή προληπτικές παρεμβάσεις. Επιπλέον, το σύστημα MBI θα παρέχει εργαλεία για αποτελεσματικό και φιλικό προς το χρήστη σχεδιασμό παιχνιδιών από τους επαγγελματίες υγείας[21].

Διαδικτυακή εφαρμογή (Web portal): Η διαδικτυακή εφαρμογή θα παρέχει διεπαφή και υποστήριξη για τους ασθενείς, τους φροντιστές, τους επαγγελματίες υγείας και το διαχειριστή του συστήματος. Θα προβάλλονται μέσω αυτής υπηρεσίες με συγκεκριμένο στόχο, ανάλογα με τις ανάγκες του ασθενούς, το ιστορικό αλλά και η παροντική κατάσταση του προσωποποιημένου τους προγράμματος αποκατάστασης.

Οι περιπτώσεις χρήσης του συστήματος έχουν παραχθεί βασισμένες στις απαιτήσεις του χρήστη για κάθε συμμετέχοντα ξεχωριστά. Για λόγους πληρότητας παρατίθενται συνολικά αυτές οι περιπτώσεις σε ξεχωριστό παράρτημα στο τέλος του βιβλίου. Για την εξαγωγή των απαιτήσεων του κάθε συμμετέχοντα ξεχωριστά χρησιμοποιήθηκαν μια σειρά από διαφορετικούς μηχανισμούς, μια σύνοψη των οποίων παρουσιάζεται παρακάτω[20]:

Ερωτηματολόγια: Αυτή η τεχνική περιλαμβάνει την υποβολή μιας λίστας συγκεκριμένων ερωτήσεων σε επιλεγμένους ενδιαφερόμενους. Κάθε ερώτηση

μπορεί να δοθεί σε ένα σύντομο πλαίσιο και απαιτεί μια σύντομη, τυποποιημένη απάντηση από μια προκαθορισμένη λίστα πιθανών απαντήσεων. Οι ενδιαφερόμενοι πρέπει απλώς να επιστρέψουν το ερωτηματολόγιο που σημειώνεται με τις απαντήσεις τους[22][23].

Συνεντεύξεις: Στην περίπτωση του συστήματος ιατρικής επιχειρησιακής νοημοσύνης χρησιμοποιήσαμε μη δομημένες συνεντεύξεις, δηλαδή συνεντεύξεις που δεν περιέχουν προκαθορισμένο σύνολο ερωτήσεων. Οι συνεντεύξεις αποτελούνται από μια ελεύθερη άτυπη συζήτηση με το ενδιαφερόμενο μέρος σχετικά με τη χρήση του προτεινόμενου συστήματος. Τα θέματα που συζητήθηκαν αφορούσαν την καταγραφή των αναγκών τους, την άποψή τους για τον προκαταρκτικό σχεδιασμό του συστήματος και πώς προτιμούν να αλληλοεπιδρούν με αυτό[23][11].

Επαναχρησιμοποίηση γνώσης: Τα συστήματα σπάνια σχεδιάζονται από το μηδέν. Οι μηχανικοί και οι ενδιαφερόμενοι φορείς τείνουν να επαναχρησιμοποιούν τις γνώσεις από προηγούμενες εμπειρίες με συναφή συστήματα. Τέτοιες γνώσεις μπορούν να αφορούν την οργάνωση, τον τομέα στον οποίο βασίζεται το πρόβλημα, το είδος των προβλημάτων που έχουν προκύψει με παρόμοια συστήματα ή ακόμα και προηγούμενες απαιτήσεις των συνιστωσών που επαναχρησιμοποιούνται στο συγκεκριμένο σύστημα. Η συστηματική επαναχρησιμοποίηση της γνώσης μπορεί να επιταχύνει σημαντικά τη διαδικασία εκπόνησης[24].

3.3 Περιγραφή περιπτώσεων χρήσης του συστήματος ιατρικής επιχειρησιακής νοημοσύνης

Οι περιπτώσεις χρήσεις περιγράφουν πως οι χρήστες και η πλατφόρμα του παιχνιδιού αλληλοεπιδρούν, έτσι ώστε να ικανοποιούν τις ανάγκες της υπηρεσίας. Το σύνολο των περιπτώσεων χρήσης παρέχει μια συστηματική περιγραφή των εργαλείων και υπηρεσιών του συστήματος, εξάγει τις απαραίτητες ενότητες λογισμικού και βοηθάει στο να βρεθεί το σύστημα αρχιτεκτονικής που εκτελεί καλύτερα αυτές τις υπηρεσίες και τα εργαλεία. Οι περιπτώσεις χρήσης αφορούν όλες τις λειτουργίες που πρέπει να εκτελέσει ένα ενεργό συστατικό του συστήματος και παρέχουν ένα απλό και λειτουργικό περίγραμμα του συστήματος, χωρίς να στέκονται σε λεπτομέρειες. Οι περιπτώσεις χρήσεις που παρουσιάζονται χρησιμοποιούν μια υψηλού επιπέδου περιγραφή, ώστε να γίνεται κατανοητό και από μη επαγγελματίες του χώρου, τι δυνατότητες και λειτουργίες παρουσιάζουν τα εργαλεία/συσκευές του συστήματος, αλλά και ποιος είναι ο ρόλος του κάθε ενός στο σύστημα[25][26][27][28].

3.3.1.1 Περιπτώσεις χρήσης κατά την εγγραφή

Τίτλος	**Εγγραφή του χρήστη από τον διαχειριστή**
Σκοπός/Στόχος	Κάθε χρήστης (Ιατρός, ασθενής η φροντιστής) θα πρέπει να εγγράφεται στο σύστημα ιατρικής επιχειρησιακής

	νοημοσύνης και με βάση τα δικαιώματα του θα μπορεί να χρησιμοποιεί τις διαθέσιμες λειτουργίες.
Επίπεδο	Υπολειτουργία
Πρωτοβάθμιος φορέας	**Διαχειριστής**
Δευτεροβάθμιος φορέας	• **Ιατρός** • **Ασθενής**
Συνθήκες	Καμία
Πραγματοποιούμενες ενέργειες	Ο διαχειριστής αποκτά πρόσβαση στο GUI του συστήματος ιατρικής επιχειρησιακής νοημοσύνης και επιλέγει την λειτουργία **Νέος Λογαριασμός.**
Βασική Ροή	1. Ο κύριος φορέας είναι ο διαχειριστής: Ο διαχειριστής εισέρχεται στη διαδικτυακή πύλη του συστήματος ιατρικής επιχειρησιακής νοημοσύνης και πιστοποιεί τον αυτό του. 2. Μέσω της διεπαφής του συστήματος, ο διαχειριστής αποκτά πρόσβαση στο αποθετήριο του συστήματος ιατρικής επιχειρησιακής νοημοσύνης, προετοιμάζει τους νέους λογαριασμούς και εγγράφει τους χρήστες στο σύστημα. 3. Ο διαχειριστής καθορίζει τις προκαταρκτικές πληροφορίες του νέου ιατρού: το ρόλο του και μία σειρά από βασικές πληροφορίες για να τον κατατάξει ανάλογα με τα προσόντα του. 4. Ο διαχειριστής εκχωρεί πρόσβαση και άδεια στον ιατρό για τη διαμόρφωση του παιχνιδιού. 5. Ο ιατρός λαμβάνει ένα email που τον ειδοποιεί ότι είναι πλέον εγγεγραμμένος στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης και μπορεί να εισέλθει σε αυτό με τον όνομα χρήστη και τον κωδικό του.
Εναλλακτική ροή	Ο πρωτοβάθμιος φορέας είναι ο ιατρός: 1. Ο ιατρός προσδιορίζει τις πληροφορίες του ασθενούς (ή του φροντιστή). 2. Ο ιατρός εγγράφει τον ασθενή (ή τον φροντιστή). 3. Ο ασθενής (ή ο φροντιστής), λαμβάνει ένα email που τον ειδοποιεί ότι είναι πλέον εγγεγραμμένος στο

	σύστημα και θα πιστοποιείται η παρουσία του με ένα όνομα χρήστη και έναν κωδικό.

Πίνακας 1 Εγγραφή του χρήστη από το διαχειριστή

Τίτλος	**Πιστοποίηση του χρήστη**
Σκοπός/Στόχος	Ο χρήστης πρέπει να πιστοποιηθεί και να κάνει log in για να εκτελέσει μόνο τις δραστηριότητες που θα του επιτραπούν.
Επίπεδο	Υπολειτουργία
Πρωτοβάθμιος φορέας	• **Ιατρός** • **Ασθενής**
Δευτεροβάθμιος φορέας	Κανένας
Συνθήκες	Ο ιατρός έχει είδη εγγραφεί από το διαχειριστή.
Πραγματοποιούμενες ενέργειες	Ο ιατρός αποκτά πρόσβαση στο GUI της διαδικτυακής πύλης του συστήματος ιατρικής επιχειρησιακής νοημοσύνης και επιλέγει τη λειτουργία **log in.**
Βασική Ροή	1. Ο ιατρός ανοίγει τη διαδικτυακή πύλη του συστήματος ιατρικής επιχειρησιακής νοημοσύνης. 2. Ο ιατρός επιλέγει τη λειτουργία log in και δίνει το όνομα χρήστη και τον κωδικό του. 3. Η διαδικτυακή πύλη του συστήματος εξουσιοδοτεί τον ιατρό και ανοίγει τη διεπαφή με τις λειτουργίες που αυτός μπορεί να χρησιμοποιήσει.
Εναλλακτική ροή	Ο ασθενής ζητά πρόσβαση: 1. Ο ασθενής ανοίγει την κονσόλα παιχνιδιών του συστήματος. 2. Η μηχανή γραφικών πραγματικού χρόνου του παιχνιδιού, εμφανίζει στον ασθενή το μενού log in. 3. Ο ασθενής κάνει log in βάζοντας το όνομα χρήστη και τον κωδικό του. 4. Η μηχανή γραφικών πραγματικού χρόνου πιστοποιεί τον ασθενή και στη συνέχεια ανοίγει μια συνεδρία παιχνιδιού.

	5. Στην περίπτωση που ο ασθενής ξεχάσει τον κωδικό του, επικοινωνεί με έναν φροντιστή για να τον βοηθήσει στην ανάκτηση του κωδικού του.

Πίνακας 2 Πιστοποίηση του χρήστη

Τίτλος	**Κατέβασμα ασκήσεων για το παιχνίδι**
Σκοπός/Στόχος	Γίνεται πρόσβαση στη βάση δεδομένων του συστήματος ιατρικής επιχειρησιακής νοημοσύνης, με σκοπό το κατέβασμα ακολουθιών από ασκήσεις και ενημέρωση της μηχανής γραφικών πραγματικού χρόνου.
Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	**Μηχανή γραφικών πραγματικού χρόνου**
Δευτεροβάθμιος φορέας	Σέρβερ βάσης δεδομένων συστήματος ιατρικής επιχειρησιακής νοημοσύνης.
Συνθήκες	Οι ασκήσεις στο σέρβερ του συστήματος έχουν ενημερωθεί.
Πραγματοποιούμενες ενέργειες	Ο ασθενής έχει κάνει log in στη μηχανή γραφικών πραγματικού χρόνου και μια καινούρια συνεδρία έχει ξεκινήσει.
Βασική Ροή	1. Η μηχανή γραφικών πραγματικού χρόνου λειτουργεί σαν client και «ζητά» να συνδεθεί στο σέρβερ της βάσης δεδομένων του συστήματος. 2. Η βάση δεδομένων του συστήματος αρχίζει την αναζήτηση. 3. Η μηχανή γραφικών πραγματικού χρόνου κάνει log in στον σέρβερ του συστήματος ιατρικής επιχειρησιακής νοημοσύνης (πιστοποίηση και πρόσβαση). 4. Ο σέρβερ του συστήματος εκτελεί έλεγχο έκδοσης (συγκρίνει τον αριθμό έκδοσης των εγκατεστημένων ασκήσεων στη μηχανή γραφικών πραγματικού χρόνου, με αυτές που είναι αποθηκεμένες στο σέρβερ του συστήματος ιατρικής επιχειρησιακής νοημοσύνης). 5. Εάν ο σέρβερ του συστήματος ιατρικής επιχειρησιακής νοημοσύνης έχει μία πιο πρόσφατη έκδοση, τότε η μηχανή γραφικών πραγματικού

	χρόνου κατεβάζει την ενημερωμένη έκδοση των ασκήσεων. 6. Η μηχανή γραφικών πραγματικού χρόνου, κάνει log out και αποσυνδέεται από το σέρβερ του συστήματος ιατρικής επιχειρησιακής νοημοσύνης. 7. Η μηχανή γραφικών πραγματικού χρόνου ενημερώνει την διαμόρφωση.
Εναλλακτική ροή	Μη ενημερωμένες ασκήσεις υπάρχουν στον σέρβερ του συστήματος ιατρικής επιχειρησιακής νοημοσύνης 1. Η μηχανή γραφικών πραγματικού χρόνου πραγματοποιεί Log out και αποσυνδέεται από το σέρβερ του συστήματος ιατρικής επιχειρησιακής νοημοσύνης. 2. Η μηχανή γραφικών πραγματικού χρόνου ξεκινά το παιχνίδι.

Πίνακας 3: Κατέβασμα ασκήσεων για το παιχνίδι

3.3.2 Περιπτώσεις χρήσης κατά την εκπαίδευση

Τίτλος	**Διαμόρφωση παιχνιδιού από τον ιατρό**
Σκοπός/Στόχος	Διαμόρφωση παραμέτρων για τις συνεδρίες εκπαίδευσης σύμφωνα με την τελευταία εκτίμηση κινδύνου πτώσεων του ασθενούς.
Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	• **Ιατρός** • **Ασθενής**
Δευτεροβάθμιος φορέας	Κανένας
Συνθήκες	Καμία
Πραγματοποιούμενες ενέργειες	Καμία
Βασική Ροή	1. Ο ιατρός αποκτά πρόσβαση στο GUI της διαδικτυακής πύλης του συστήματος και ανοίγει τη λειτουργία **Διαμόρφωση παιχνιδιού**.

	2. Ο ιατρός αποκτά πρόσβαση στο αποθετήριο όπου βρίσκονται οι στάσεις των ασκήσεων. 3. Ο ιατρός χρησιμοποιεί τις λειτουργίες σχεδιασμού του παιχνιδιού που του παρέχονται από το σύστημα, για να επιλέξει τις στάσεις και να «χτίσει» το παιχνίδι σύμφωνα με τις απαιτήσεις του πλάνου αποκατάστασης του ασθενούς. 4. Ο ιατρός θέτει το βαθμό εκπλήρωσης του κάθε βήματος στο παιχνίδι. 5. Ο ιατρός συνδέει τις συσκευές και τους αισθητήρες με τον ασθενή.
Εναλλακτική ροή	Ο ιατρός επιλέγει τη συνεδρία εκπαίδευσης και αξιολόγησης • Ο ιατρός επιλέγει συγκεκριμένες ασκήσεις που έχουν στόχο να αξιολογήσουν τις χωροχρονικές παραμέτρους της κινηματικής κατάστασης του ασθενούς. • Ο ιατρός χρησιμοποιεί τις λειτουργίες σχεδιασμού του παιχνιδιού για να επιλέξει ασκήσεις και να «χτίσει» το παιχνίδι σύμφωνα με το πλάνο εκτίμησης κίνησης του ασθενούς. • Ο ιατρός συνδέει τις συσκευές και τους αισθητήρες με τον ασθενή.

Πίνακας 4 Διαμόρφωση ασκήσεων από το γιατρό

Τίτλος	**Προετοιμασία παιχνιδιού**
Σκοπός/Στόχος	Ο ασθενής αρχίζει τη συνεδρία εκπαίδευσης απλά πατώντας ένα κουμπί. Το σύστημα επαληθεύει ότι όλες οι συσκευές είναι ενεργές και έτοιμες προς χρήση.
Επίπεδο	Λειτουργία
Πρωτοβάθμιος φορέας	• **Ασθενής**

	• **Μηχανή γραφικών πραγματικού χρόνου**
Δευτεροβάθμιος φορέας	**Σύστημα ιατρικής επιχειρησιακής νοημοσύνης.**
Συνθήκες	Καμία
Πραγματοποιούμενες ενέργειες	Ο ασθενής επιλέγει τη λειτουργία log in
Βασική Ροή	1. Ταυτοποίηση του ασθενούς 2. Ο ασθενής αλληλοεπιδρά με τη μηχανή γραφικών πραγματικού χρόνου του παιχνιδιού και επιλέγει την « αρχικοποίηση παιχνιδιού». 3. Η μηχανή γραφικών πραγματικού χρόνου κατεβάζει από τη βάση δεδομένων του συστήματος την ενημερωμένη έκδοση του παιχνιδιού (πρόγραμμα και παράμετροι παιχνιδιού) 4. Η μηχανή γραφικών πραγματικού χρόνου εντοπίζει ενεργές συσκευές και αισθητήρες και επαληθεύει ότι είναι ανοιχτοί και έτοιμοι προς χρήση. 5. Ο ασθενής λαμβάνει μια ειδοποίηση από τη μηχανή γραφικών πραγματικού χρόνου για την κατάσταση λειτουργίας της πλατφόρμας. 6. Η μηχανή γραφικών πραγματικού χρόνου «περιμένει» από τον ασθενή να πατήσει το κουμπί έναρξης.
Εναλλακτική ροή	Η μηχανή γραφικών πραγματικού χρόνου εντοπίζει συσκευές ή αισθητήρες που βρίσκονται εκτός λειτουργίας. • Η μηχανή γραφικών πραγματικού χρόνου βγάζει ένα «μήνυμα σφάλματος» στην οθόνη του ασθενούς και στέλνει ένα σήμα συναγερμού στο σύστημα μαζί με μια αναφορά σφάλματος για περαιτέρω ανάλυση.

Πίνακας 5 Προετοιμασία του παιχνιδιού

Τίτλος	**Εκτέλεση του παιχνιδιού**
Σκοπός/Στόχος	Ο ασθενής εκτελεί τις ασκήσεις υπό την επίβλεψη του ελεγκτή παιχνιδιού.

Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	• **Ασθενής** • **Μηχανή γραφικών πραγματικού χρόνου**
Δευτεροβάθμιος φορέας	Κανένας
Συνθήκες	Καμία
Πραγματοποιούμενες ενέργειες	Ο ασθενής πατάει το κουμπί έναρξης.
Βασική Ροή	1. Ο ελεγκτής παιχνιδιού ξεκινά την συνεδρία παιχνιδιού. 2. Ο ελεγκτής παιχνιδιού ζητά τα δεδομένα των αισθητήρων από τον sensor listener . 3. Ο ασθενής λαμβάνει σήματα ανατροφοδότησης υπολογισμένα από τον ελεγκτή παιχνιδιού. 4. Όταν το παιχνίδι ολοκληρωθεί επιτυχώς ο ελεγκτής παιχνιδιού τερματίζει τη συνεδρία. 5. Ο ασθενής λαμβάνει ένα συνολικό σκορ από τον ελεγκτή του παιχνιδιού. 6. Όταν ο ασθενής είναι έτοιμος, πατάει το κουμπί έναρξης για την επόμενη συνεδρία, αλλιώς τερματίζει το παιχνίδι.
Εναλλακτική ροή	Ο ελεγκτής παιχνιδιού τερματίζει την εκτέλεση του παιχνιδιού, όταν λάβει ένα σήμα διακοπής (είτε από κάποιο συναγερμό, είτε από μια δυσλειτουργία ενός αισθητήρα/μιας συσκευής).

Πίνακας 6 Εκτέλεση του παιχνιδιού

Τίτλος	**Αίτηση των δεδομένων του αισθητήρα**
Σκοπός/Στόχος	Παρακολούθηση και καταγραφή της επίδοσης των ασθενών κατά τη διάρκεια των ασκήσεων.
Επίπεδο	Λειτουργία
Πρωτοβάθμιος φορέας	**Sensor listener**

Δευτεροβάθμιος φορέας	**Αποθήκευση τοπικών δεδομένων**
Συνθήκες	Ο ασθενής ακολουθεί τις οδηγίες του παιχνιδιού και εκτελεί την ακολουθία των ασκήσεων.
Πραγματοποιούμενες ενέργειες	Ο **sensor listener** καταγράφει δεδομένα.
Βασική Ροή	1. Ο sensor listener συλλέγει πληροφορίες από: • Τον αισθητήρα βάθους • IMU δεδομένα • Άλλους αισθητήρες (υγρασία, καρδιακοί παλμοί κτλ.) 2. Ο sensor listener προ επεξεργάζεται τα δεδομένα. 3. Τα δεδομένα του KINECT και τα δεδομένα από το επιταχυνσιόμετρο, γυροσκόπιο και μαγνητόμετρο αποθηκεύονται στην μονάδα αποθήκευσης του τοπικού υπολογιστή για επεξεργασία σε πραγματικό χρόνο. 4. Δεδομένα βίντεο καθώς και άλλα δεδομένα αποθηκεύονται στο τοπικό αποθετήριο του συστήματος ιατρικής επιχειρησιακής νοημοσύνης και «ανεβαίνουν» στην κεντρική βάση δεδομένων του συστήματος αμέσως μετά τον τερματισμό της συνεδρίας.
Εναλλακτική ροή	Καμία

Πίνακας 7 Αίτηση των δεδομένων του αισθητήρα

Τίτλος	**Αίτημα σήματος ανάδρασης**
Σκοπός/Στόχος	Επεξεργασία των δεδομένων από τους αισθητήρες του συστήματος ιατρικής επιχειρησιακής νοημοσύνης, για ανάδραση σε πραγματικό χρόνο κατά τη διάρκεια της συνεδρίας του παιχνιδιού.
Επίπεδο	Λειτουργία
Πρωτοβάθμιος φορέας	**Μηχανή γραφικών πραγματικού χρόνου**

Δευτεροβάθμιος φορέας	Κανένας
Συνθήκες	Κανένας
Πραγματοποιούμενες ενέργειες	Η παραγόμενη ανάδραση ενεργοποιείται αυτόματα από τη μηχανή γραφικών πραγματικού χρόνου.
Βασική Ροή	1. Ο ελεγκτής παιχνιδιού λαμβάνει δεδομένα για τη στάση του σώματος από το KINECT. 2. Ενημερώνονται τρισδιάστατα avatars με τη στάση του σώματος. 3. Υπολογίζεται η διαφορά μεταξύ της ιδανικής στάσης του σώματος και της πραγματικής στάσης σώματος και προκύπτει το σκορ στην άσκηση. 4. Παρέχονται σήματα ανάδρασης με δόνηση στον ασθενή βασισμένα στην υπολογισμένη διαφορά. 5. Εμφανίζεται στην οθόνη το σκορ που πέτυχε ο ασθενής στην άσκηση.
Εναλλακτική ροή	Καμία

Πίνακας 8 Αίτημα σήματος ανάδρασης

Τίτλος	**Ειδοποιήσεις περιεχομένου**
Σκοπός/Στόχος	Η μηχανή γραφικών πραγματικού χρόνου «ζητά» κατά τη διάρκεια του παιχνιδιού σε πραγματικό χρόνο πληροφορίες γενικού περιεχομένου: καρδιακός ρυθμός, θερμοκρασία και υγρασία. Αυτή η πληροφορία χρησιμοποιείται για να αξιολογηθεί η κατάσταση του ασθενούς και αν χρειαστεί να ενεργοποιηθεί κάποιος συναγερμός.
Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	**Μηχανή γραφικών πραγματικού χρόνου**
Δευτεροβάθμιος φορέας	Διαδικτυακή πύλη του συστήματος ιατρικής επιχειρησιακής νοημοσύνης.
Συνθήκες	Καμία
Πραγματοποιούμενες ενέργειες	Καμία

Βασική Ροή	1. Η μηχανή γραφικών πραγματικού χρόνου αναζητά δεδομένα περιεχομένου από το sensor listener. 2. Ο sensor listener στέλνει τα ζητούμενα δεδομένα στη μηχανή γραφικών πραγματικού χρόνου. 3. Η μηχανή γραφικών πραγματικού χρόνου επεξεργάζεται τα δεδομένα με βάση ένα σετ κανόνων. 4. Η μηχανή γραφικών πραγματικού χρόνου αυξάνει τους συναγερμούς εάν οι τιμές των αισθητήρων υπερβούν τα όρια.
Εναλλακτική ροή	Καμία

Πίνακας 9 Ειδοποιήσεις περιεχομένου

Τίτλος	**Εκτίμηση της κινηματικής ανάλυσης**
Σκοπός/Στόχος	Τα δεδομένα από τις προπονήσεις επεξεργάζονται και αναλύονται off-line και παράγονται χρήσιμα αποτελέσματα στο σύστημα DSS.
Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	• **Εφαρμογή κινηματικής ανάλυσης** • **Εφαρμογή DSS του συστήματος ιατρικής επιχειρησιακής νοημοσύνης**
Δευτεροβάθμιος φορέας	Διαδικτυακή πύλη συστήματος ιατρικής επιχειρησιακής νοημοσύνης.
Συνθήκες	Το σύστημα επιχειρησιακής νοημοσύνης έχει τελειώσει το ανέβασμα των δεδομένων από την τελευταία συνεδρία παιχνιδιού.
Πραγματοποιούμενες ενέργειες	Καμία
Βασική Ροή	1. Η εφαρμογή των MBI-DSS ενεργοποιεί την εφαρμογή κινηματικής ανάλυσης. 2. Η εφαρμογή κινηματικής ανάλυσης προσπελαύνει την βάση δεδομένων του MBI και ανακτά τις εντοπισμένες σκελετικές αρθρώσεις της τελευταίας συνεδρίας παιχνιδιού.

	3. Η εφαρμογή κινηματικής ανάλυσης εκτιμά τις χωροχρονικές τιμές. 4. Η εφαρμογή κινηματικής ανάλυσης αποθηκεύει τις εκτιμώμενες χωροχρονικές τιμές στη βάση δεδομένων του MBI. 5. Η εκτίμηση της κινηματικής ανάλυσης τερματίζει επιτυχώς.
Εναλλακτική ροή	Καμία

Πίνακας 10 Εκτίμηση της κινηματικής ανάλυσης

Τίτλος	**Εκτίμηση κινδύνου πτώσης**
Σκοπός/Στόχος	Ο ιατρός, με τη βοήθεια της εφαρμογής εκτίμησης κινδύνου πτώσης, διαπιστώνει τον κίνδυνο πτώσης των ασθενών.
Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	• **Εφαρμογή εκτίμησης κινδύνου πτώσης/MBI** • **Ιατρός**
Δευτεροβάθμιος φορέας	Διαδικτυακή πύλη συστήματος
Συνθήκες	Η κινηματική ανάλυση έχει τερματιστεί με επιτυχία
Πραγματοποιούμενες ενέργειες	Καμία
Βασική Ροή	1. Η εφαρμογή MBI-DSS ενεργοποιεί την εφαρμογή κινδύνου πτώσης. 2. Η εφαρμογή κινδύνου πτώσης ανακτά τα χωροχρονικά αποτελέσματα που βρίσκονται αποθηκευμένα στη βάση δεδομένων του συστήματος ιατρικής επιχειρησιακής νοημοσύνης. 3. Επεξεργασία των χωροχρονικών αποτελεσμάτων. Ο αλγόριθμος εκτίμησης κινδύνου πτώσης διακρίνει τα συμπωματικά λειτουργικά χαρακτηριστικά από τα μη λειτουργικά χαρακτηριστικά, σε κάθε συνεδρία και τα κατηγοριοποιεί σε επίπεδα κινδύνου.

	4. Αποθηκεύει στη βάση δεδομένων του MBI το επίπεδο κινδύνου πτώσης. 5. Η βάση δεδομένων του MBI παράγει ως αποτέλεσμα εξόδου της εφαρμογής κινδύνου πτώσης, μια ετικέτα με το επίπεδο κινδύνου πτώσης.
Εναλλακτική ροή	Καμία

Πίνακας 11 Εκτίμηση κινδύνου πτώσης

Τίτλος	**Επιθεώρηση της εκτίμησης κινδύνου πτώσης**
Σκοπός/Στόχος	Ο ιατρός, δέχεται ή απορρίπτει το αποτέλεσμα της εκτίμησης κινδύνου πτώσης.
Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	• **MBI-DSS** • **Ιατρός**
Δευτεροβάθμιος φορέας	Διαδικτυακή πύλη συστήματος
Συνθήκες	Η κινηματική ανάλυση έχει τερματιστεί επιτυχώς.
Πραγματοποιούμενες ενέργειες	Καμία
Βασική Ροή	1. Ο ιατρός κάνει log in στη διαδικτυακή πύλη του συστήματος. 2. Ο ιατρός εισάγει το αρχείο διαχείρισης του ασθενούς. 3. Ο ιατρός αποκτά πρόσβαση στο MBI-DSS και ζητά το αποτέλεσμα κινδύνου πτώσης. 4. Ο ιατρός ζητά πρόσβαση στο ιατρικό ιστορικό του ασθενούς. 5. Ο ιατρός εξετάζει τις πληροφορίες και δέχεται η απορρίπτει το αποτέλεσμα εκτίμησης κινδύνου πτώσης.
Εναλλακτική ροή	Καμία

Πίνακας 12 Επιθεώρηση της εκτίμησης κινδύνου πτώσης

Τίτλος	**Σχεδιασμός πλάνου αναμόρφωσης**
Σκοπός/Στόχος	Ο ιατρός υποβοηθείται, από τη νοημοσύνη του DSS, για να χτίσει ένα πλάνο αποκατάστασης ασθενών.
Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	• **Εφαρμογή MBI/DSS** • **Ιατρός**
Δευτεροβάθμιος φορέας	Διαδικτυακή πύλη συστήματος
Συνθήκες	• Ο ιατρός κάνει log in στη διαδικτυακή πύλη του συστήματος. • Το MBI/DSS έχει ενημερώσει το αποτέλεσμα της εκτίμησης κινδύνου πτώσης.
Πραγματοποιούμενες ενέργειες	Καμία
Βασική Ροή	1. Ο ιατρός ξεκινά την ενότητα του DSS 2. Το DSS ανακτά από τη βάση δεδομένων του MBI: a) Τα αποτελέσματα της εκτίμησης κινδύνου πτώσης. b) Τα σκορ του τελευταίου παιχνιδιού. 3. Ο αλγόριθμος του DSS παράγει ένα προτεινόμενο πρόγραμμα παιχνιδιού μαζί με τις παραμέτρους του. 4. Ο ιατρός, δέχεται, απορρίπτει ή τροποποιεί το προτεινόμενο πρόγραμμα παιχνιδιού. 5. Το ενημερωμένο σετ των ασκήσεων καθώς και το πλάνο αποκατάστασης ασθενών, αποθηκεύονται στη βάση δεδομένων του MBI.
Εναλλακτική ροή	Καμία

Πίνακας 13 Σχεδιασμός πλάνου αναμόρφωσης

3.3.3 Περιπτώσεις χρήσης κατά τη διαχείριση αρχείων

Τίτλος	**Επιλογή λογαριασμού ασθενούς**

Σκοπός/Στόχος	Επιλογή του φάκελου του ασθενούς από τη βάση δεδομένων των εγγεγραμμένων χρηστών του συστήματος.
Επίπεδο	Λειτουργία
Πρωτοβάθμιος φορέας	**Ιατρός**
Δευτεροβάθμιος φορέας	Διαδικτυακή πύλη συστήματος
Συνθήκες	Αναγνώριση του ιατρού
Πραγματοποιούμενες ενέργειες	Ο ιατρός επιλέγει τη λειτουργία **«επιλογή χρήστη»**
Βασική Ροή	1. Ο ιατρός μέσω της διαδικτυακής πύλης του συστήματος εντοπίζει τη λίστα των εγγεγραμμένων χρηστών στους οποίους έχει εξουσιοδότηση πρόσβασης και επιλέγει το όνομα του ασθενούς που τον ενδιαφέρει. 2. Η διαδικτυακή πύλη ελέγχει τις άδειες του ιατρού. 3. Η διαδικτυακή πύλη εμφανίζει ένα μενού με περιεχόμενο στο οποίο ο ιατρός είναι εξουσιοδοτημένος να διαβάσει και να γράψει: • Ιατρικό ιστορικό • Συνεδρίες • Προγράμματα παιχνιδιών
Εναλλακτική ροή	Τα διαπιστευτήρια του ιατρού δε του δίνουν τη απαραίτητη πρόσβαση στις παραμέτρους του προγράμματος παιχνιδιού. Η διαδικτυακή πύλη ανοίγει μενού με περιεχόμενο στο οποίο ο ιατρός είναι εξουσιοδοτημένος μόνο να διαβάσει: • Ιατρικό ιστορικό • Συνεδρίες • Προγράμματα παιχνιδιών

Πίνακας 14 Επιλογή λογαριασμού ασθενούς

Τίτλος	**Διαχείριση του ιατρικού φακέλου**
Σκοπός/Στόχος	Επιλογή του φακέλου του ασθενούς από τη βάση δεδομένων εγγεγραμμένων χρηστών του MBI
Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	**Ιατρός**
Δευτεροβάθμιος φορέας	Διαδικτυακή πύλη συστήματος
Συνθήκες	Ταυτοποίηση του ιατρού
Πραγματοποιούμενες ενέργειες	Ο ιατρός έχει εισέλθει στην directory του ασθενούς
Βασική Ροή	1. Επιλέγει «ιατρικό φάκελο» 2. Επιλέγει διάβασμα ιατρικού φακέλου και περιήγηση μέσω της τρέχουσας κατάστασης ή του ιστορικού του ασθενούς.
Εναλλακτική ροή	Επιλέγει εγγραφή ιατρικού αρχείου • Η βάση δεδομένων του MBI ελέγχει τις άδειες. Ένα οι άδειες έχουν χορηγηθεί, τότε ανοίγει το ιατρικό αρχείο σε μορφή επεξεργασίας. Αλλιώς εμφανίζεται μήνυμα απαγόρευσης πρόσβασης. Επιλέγει εξαγωγή φακέλου. Ο ιατρός πλοηγείται μέσω της βάσης δεδομένων του MBI στα αρχεία του ασθενούς και επιλέγει το επιθυμητό αρχείο προς εξαγωγή.

Πίνακας 15 Διαχείριση του ιατρικού φακέλου

Τίτλος	**Συμπλήρωση του ηλεκτρονικού ημερολογίου**
Σκοπός/Στόχος	Χρήση του ηλεκτρονικού ημερολογίου για τον προγραμματισμό τον συνεδριών εκπαίδευσης του ασθενούς.
Επίπεδο	Υπηρεσία
Πρωτοβάθμιος φορέας	**Ιατρός**
Δευτεροβάθμιος φορέας	Διαδικτυακή πύλη συστήματος
Συνθήκες	Καμία

Πραγματοποιούμενες ενέργειες	Η λειτουργία **«ηλεκτρονικό ημερολόγιο»** έχει επιλεγεί.
Βασική Ροή	1. Επιλογή του φακέλου του ασθενούς. 2. Επιλογή του τρόπου προβολής του ημερολογίου (ημερήσια, εβδομαδιαία, μηνιαία). 3. Συμβάντα. 4. Ρύθμιση ώρας προγράμματος για ειδοποιήσεις.
Εναλλακτική ροή	Επιλογή του φακέλου του ιατρού (ο ιατρός κανονίζει το πρόγραμμα του) 1. Επιλογή του τρόπου προβολής του ημερολογίου (ημερήσια, εβδομαδιαία, μηνιαία). 2. Συμβάντα. 3. Ρύθμιση ώρας προγράμματος για ειδοποιήσεις.

Πίνακας 16 Συμπλήρωση του ηλεκτρονικού ημερολογίου

Τίτλος	**Ενημέρωση του σέρβερ του MBI**
Σκοπός/Στόχος	Ανέβασμα (από το τοπικό αποθετήριο) των συγκεντρωμένων δεδομένων κατά τη διάρκεια της τελευταίας συνεδρίας παιχνιδιού στη βάση δεδομένων του MBI.
Επίπεδο	Λειτουργία
Πρωτοβάθμιος φορέας	**Ιατρός**
Δευτεροβάθμιος φορέας	Διαδικτυακή πύλη συστήματος
Συνθήκες	Καμία
Πραγματοποιούμενες ενέργειες	Η συνεδρία παιχνιδιού έχει ολοκληρωθεί
Βασική Ροή	1. Η συνεδρία παιχνιδιού ολοκληρώνεται και στέλνει σήμα τερματισμού στη μηχανή γραφικών πραγματικού χρόνου. 2. Η μηχανή γραφικών πραγματικού χρόνου λειτουργεί σαν client ζητά σύνδεση με τη βάση δεδομένων του σέρβερ του MBI.

	3. Η βάση δεδομένων του MBI ξεκινά την ανίχνευση. 4. Η μηχανή γραφικών πραγματικού χρόνου κάνει log in στον server του MBI (ταυτοποίηση και πρόσβαση). 5. Η μηχανή γραφικών πραγματικού χρόνου ζητά πρόσβαση εγγραφής στο λογαριασμό του ασθενούς. 6. Η βάση δεδομένων εξουσιοδοτεί τη μηχανή γραφικών πραγματικού χρόνου και αποδέχεται το αίτημα. 7. Η μηχανή γραφικών πραγματικού χρόνου ανεβάζει τα δεδομένα από τη συνεδρία παιχνιδιού. 8. Η μηχανή γραφικών πραγματικού χρόνου κάνει log out και αποσυνδέεται από το server του MBI.
Εναλλακτική ροή	Καμία

Πίνακας 17 Ενημέρωση του σέρβερ του MBI

3.3.4 Ανάπτυξη νέας περίπτωσης χρήσης

Η χρήση των αφηγήσεων αποδεικνύεται πολύ αποτελεσματική στα πρώιμα στάδια της διαδικασίας των λειτουργικών απαιτήσεων, στο να συγκεντρώσει χρήσιμες πληροφορίες μέσα από συγκεκριμένα παραδείγματα για το πως τρέχουν τα πράγματα και αλληλοεπιδρούν με το ισχύον σύστημα, η πως θα έπρεπε να λειτουργούν σε μια μελλοντική έκδοση. Ένα σενάριο που αποτελείται από περιπτώσεις χρήσης απεικονίζει μια τυπική ακολουθία των αλληλεπιδράσεων μεταξύ των συνιστωσών του συστήματος και των ενδιαφερόμενων μερών. Ισοδυναμεί με μια δομημένη αφήγηση που καλύπτει τα ποιος, τι και πώς. Κατά συνέπεια, το σενάριο που παρουσιάζεται παρακάτω, περιγράφει μια σειρά από υψηλού επιπέδου αλληλεπιδράσεις του συστήματος που υποδηλώνουν πως επιτυγχάνονται οι στόχοι του συστήματος [29][26][28].

Το σενάριο παρουσιάζεται στον πίνακα 18. Η πρώτη στήλη του πίνακα αφορά τη σειρά ακολουθίας των περιπτώσεων χρήσης. Οι επόμενες τρεις στήλες αφορούν τα μέρη που συμμετέχουν στην υπόθεση χρήσης. Τα μέρη μπορεί να είναι είτε άτομα είτε υποσυστήματα του συστήματος. Η πρώτη από αυτές τις τρεις στήλες πάντα θα αναφέρεται στους ασθενείς, η δεύτερη στον ιατρό και η τρίτη στήλη θα αναφέρεται σε ένα ή περισσότερα από τα υπόλοιπα μέρη (σε κάθε διαφορετικό βήμα το όνομα του μέρους που θα συμμετέχει θα υποδηλώνεται με έντονα γράμματα). Η τελευταία στήλη του πίνακα 18, θα αφορά την ταυτότητα της περίπτωσης χρήσης και θα δίνεται μια σύντομη περιγραφή (όλες οι περιπτώσεις χρήσης έχουν παρουσιαστεί αναλυτικά στην προηγούμενη ενότητα). Ο αριθμός μέσα στην παρένθεση (δίπλα από το

αναγνωριστικό του κάθε μέρους), υποδηλώνει τη χρονική ακολουθία των βημάτων που εκτελούνται κατά τη διάρκεια των περιπτώσεων χρήσης.

	Μέρη			**Πλατφόρμα συστήματος**
Χρονολογική σειρά των περιπτώσεων χρήσης	**Ασθενής**	**Ιατρός**	**Άλλα μέρη (έντονη γραμματοσειρά)**	**Περιπτώσεις χρήσης**
1		(2) Ο ιατρός λαμβάνει email με το όνομα χρήστη και τον κωδικό	(1) Ο **διαχειριστής** εγγράφει τον ιατρό	Εγγραφή του χρήστη από το διαχειριστή
2		Ταυτοποίηση και είσοδος στο σύστημα		Ταυτοποίηση του χρήστη
3	(2) Ο ασθενής λαμβάνει το όνομα χρήστη και τον κωδικό κατά την πρώτη επίσκεψη στο ιατρείο		(1) Ο διαχειριστής εγγράφει τον ασθενή και τον πλησιέστερο συγγενή του	Εγγραφή του χρήστη από το διαχειριστή
4	Ταυτοποίηση και είσοδος στο σύστημα			Ταυτοποίηση του χρήστη
5		Ανοίγει τη διαδικτυακή πύλη, επιλέγει και αποκτά πρόσβαση το λογαριασμό		Επιλέγει το λογαριασμό του ασθενούς

		του ασθενούς		
6		Παίρνει πληροφορίες για την παρούσα και προγενέστερη κατάσταση του ασθενούς		Διαχείριση του φακέλου του ασθενούς
7			(1) Η **βάση δεδομένων του MBI** έχει ανεβάσει και αποθηκεύσει επιτυχώς τα δεδομένα από την τελευταία συνεδρία. (2) Το **DSS** ξεκινά την εφαρμογή εκτίμησης κινδύνου πτώσης. (3) Το **FRA** ενεργοποιεί την εφαρμογή εκτίμησης κινηματικής ανάλυσης (4) Το **FRA** επεξεργάζεται δεδομένα χωροχρονικών παραμέτρων που παράγονται από την εκτίμηση της κινηματικής ανάλυσης και τα	Εκτίμηση κινδύνου πτώσης

			συγκρίνει με τις προηγούμενες συνεδρίες (5) Το **FRA** διαχωρίζει από τη μία συνεδρία παρακολούθησης στην άλλη, συμπωματικά από μη συμπωματικά λειτουργικά χαρακτηριστικά και τα κατηγοριοποιεί σε επίπεδα κινδύνου (6) Το **FRA** υπολογίζει μια τιμή κινδύνου πτώσης	
8		(1) Ανοίγει την εφαρμογή εκτίμησης πτώσης στη διαδικτυακή πύλη του συστήματος (2) Επιθεωρεί το FRA και δέχεται ή απορρίπτει το περιεχόμενο του	(8) Το νέο περιεχόμενο του FRA αποθηκεύεται στη **βάση δεδομένων του MBI**	Επισκόπηση της εκτίμησης κινδύνου πτώσης
9		(1) Ξεκινά τη διαδικασία του DSS	(2) Η **εφαρμογή του DSS** ανακτά από τη βάση δεδομένων το	Σχεδιασμός πλάνου

			σκορ της τελευταίας συνεδρίας παιχνιδιού και το περιεχόμενο του κινδύνου πτώσης (3) Το **DSS** επεξεργάζεται το αποτέλεσμα και προτείνει ένα πρόγραμμα παιχνιδιού και τις παραμέτρους του (4) Το προτεινόμενο πρόγραμμα παιχνιδιού με τις παραμέτρους του αποθηκεύεται από το **DSS** στη **βάση δεδομένων** του **MBI**	αποκατάστασης
10		(1) Επιλέγει διαμόρφωση λειτουργιών παιχνιδιού στη διαδικτυακή πύλη του συστήματος (2) Επιλέγει «παιχνίδι εκπαίδευσης		Διαμόρφωση παιχνιδιού

		και εκτίμησης» (3)Σχεδιάζει την ακολουθία του παιχνιδιού: ασκήσεις και βαθμός εκπλήρωσης (4) Αποθηκεύει τα παιχνίδια στη βάση δεδομένων του MBI		
11	(1) Ξεκινά μια νέα συνεδρία. (4) Λαμβάνει μια ειδοποίηση επιβεβαίωσης από τη μηχανή γραφικών πραγματικού χρόνου για τη λειτουργική κατάσταση του συστήματος (5) Διαβάζει στη διεπαφή εκπαιδευόμενου πληροφορίες για: αντικείμενο της εκπαίδευσης, τύπο επόμενης άσκησης, διάρκεια, επίπεδο δυσκολίας		(2) **Η μηχανή γραφικών πραγματικού χρόνου** κατεβάζει αυτόματα από τη βάση δεδομένων του MBI την ενημερωμένη έκδοση του παιχνιδιού με τις ρυθμίσεις του. (3) Η **μηχανή γραφικών πραγματικού χρόνου** επικοινωνεί με την πλατφόρμα υλικού του συστήματος και πιστοποιεί ότι οι συσκευές και οι αισθητήρες είναι	Αρχικοποίηση παιχνιδιού

			ρυθμισμένοι και έτοιμοι προς χρήση και στέλνει μήνυμα επιβεβαίωσης στον ασθενή (6) **Η μηχανή γραφικών πραγματικού χρόνου** περιμένει μέχρις ότου ο ασθενής πατήσει το κουμπί έναρξης	
12	(1) Ανοίγει παράθυρο τηλεκπαίδευσης στην πλατφόρμα GUI του συστήματος (2) Ζητά πληροφορίες από την εφαρμογή τηλεκπαίδευσης για την τρέχουσα συνεδρία παιχνιδιού (5) Αποχωρεί από το παράθυρο τηλεκπαίδευσης		(3) Η **Εφαρμογή τηλεκπαίδευσης** καταδεικνύει τους μαθησιακούς στόχους και περιγράφει την άσκηση και το βαθμό δυσκολίας (4) Η **Εφαρμογή τηλεκπαίδευσης** καταδεικνύει μια ακολουθία εικόνων της άσκησης που θα εκτελεστεί	Τηλεκπαίδευση
13	(1) Πατάει το κουμπί έναρξης. (5) Λαμβάνει ανατροφοδότηση από τον		(2) Ο **ελεγκτής παιχνιδιού** ξεκινά μια συνεδρία παιχνιδιού.	Εκτέλεση του παιχνιδιού και ολοκλήρωση

	ελεγκτή παιχνιδιού.		(3) Ο **sensor listener** τα δεδομένα των αισθητήρων του συστήματος (4) Ο **ελεγκτής παιχνιδιού** λαμβάνει δεδομένα σε πραγματικό χρόνο από τον sensor listener (6) Εάν εμφανιστεί κάποια ειδοποίηση εξαιτίας μιας κακής εκτέλεσης των ασκήσεων το παιχνίδι τερματίζει αυτόματα (7) Ο **ελεγκτής παιχνιδιού** τερματίζει τη συνεδρία παιχνιδιού μέσα στον προκαθορισμένο χρόνο (εάν δεν έχει εμφανιστεί κάποια ειδοποίηση διακοπής) (8) Ο **ελεγκτής παιχνιδιού** ξεκινά την επόμενη συνεδρία παιχνιδιού σύμφωνα με το	

			πρόγραμμα του παιχνιδιού	
14			(1) Η **μηχανή γραφικών πραγματικού χρόνου** αντιμετωπίζει ένα σήμα τερματισμού (2) Η **μηχανή γραφικών πραγματικού χρόνου** κάνει Log in στον σέρβερ του MBI (3) Η **μηχανή γραφικών πραγματικού χρόνου** ανεβάζει τα δεδομένα των συνεδριών παιχνιδιού (4) Η **μηχανή γραφικών πραγματικού χρόνου** κάνει log out και αποσυνδέεται από το σέρβερ του MBI	Ενημέρωση του σέρβερ του MBI
15			(1) Η **εφαρμογή DSS** ενεργοποιεί την εφαρμογή κινηματικής ανάλυσης (2) Η **εφαρμογή κινηματικής ανάλυσης** αποκτά	Κινηματική ανάλυση

			πρόσβαση στη βάση δεδομένων του MBI και ανακτά τις σκελετικές αρθρώσεις που έχουν αποτυπωθεί από την τελευταία συνεδρία παιχνιδιού (3) Η **εφαρμογή κινηματικής ανάλυσης** εκτιμά τις χωροχρονικές τιμές (4) Η **εφαρμογή κινηματικής ανάλυσης** αποθηκεύει τις εκτιμώμενες τιμές στη βάση δεδομένων του MBI (5) Η **εκτίμηση κινηματικής ανάλυσης** τερματίζει επιτυχώς	

Πίνακας 18 Περιγραφή σεναρίου περιπτώσεων χρήσης βασικών λειτουργιών του συστήματος

Κεφάλαιο 4ο

Ασφάλεια του συστήματος ιατρικής επιχειρησιακής νοημοσύνης

4.1 Η ασφάλεια σε ένα σύστημα πληροφορικής

Η δυνατότητα να αναγνωρίζεται με σαφήνεια, να πιστοποιείται, να επιβεβαιώνεται και να παρακολουθείται ποιος ή τι αποκτά πρόσβαση στα στοιχεία ενός οργανωμένου συστήματος πληροφορικής είναι απαραίτητη για την προστασία του συστήματος αυτού από απειλές και από άλλες αδυναμίες του. Ο διαχωρισμός είναι το βασικό συστατικό κάθε ασφαλούς συστήματος κι βασίζεται στην ικανότητα του ν δημιουργεί όρια μεταξύ των οντοτήτων που πρέπει να προστατευτούν και εκείνων που δεν πρέπει να είναι εμπιστεύσιμες[30]–[32].

4.1.1 Εμπιστοσύνη

Η εμπιστοσύνη σ ένα τέτοιο περιβάλλον εξαρτάται έντονα από το επιλεγόμενο μοντέλο εφαρμογής του συστήματος, όσο η κατοχή των δεδομένων κι των εφαρμογών εξωτερικεύεται κι παραδίδεται εκτός του αυστηρού ελέγχου του κάτοχου. Στην περίπτωση ενός δημοσίου ή συμμετοχικού συστήματος, ο έλεγχος παραδίδεται στον οργανισμό που κατέχει την υποδομή[33].

Όταν αναπτύσσεται ένα δημόσιο σύστημα, ο έλεγχος παραδίδεται στον ιδιοκτήτη της υποδομής για να επιβάλλει μια ικανοποιητική πολιτική ασφάλειας η οποία εγγυάται το γεγονός πως λαμβάνονται τα καταλληλά μέτρα ασφαλείας για να βεβαιωθεί η μείωση ή και εξάλειψη πιθανού κινδύνου. Το γεγονός αυτό διεγείρει από μόνο του έναν αριθμό από κινδύνους και απειλές, με δεδομένο ότι η ασφάλεια σχετίζεται με την εμπιστοσύνη στις διεργασίες και την υπολογιστική βάση που υιοθετείται από τον ιδιοκτήτη του συστήματος.

Είναι πολύ σημαντικό να γίνει διαφοροποίηση μεταξύ των μοντέλων εφαρμογής, ως ιδιωτικό σύστημα πληροφορικής, του οποίου η λειτουργία και η διαχείριση προϋποθέτει έναν ιδιωτικό οργανισμό και δεν εγείρει νέα ζητήματα ασφαλείας, αφού η εμπιστοσύνη υπάρχει εντός του οργανισμού. Σε μια τέτοια περίπτωση, ο ιδιοκτήτης της υποδομής παραμένει κάτοχος των δεδομένων και των διεργασιών[33][34].

4.1.2 Αναγνώριση των απειλών

Το δίχως άλλο, η ασφάλιση ενός συστήματος πληροφορικής περιλαμβάνει την αναγνώριση μοναδικών απειλών και προβλημάτων, τα οποί πρέπει να ρυθμιστούν εφαρμόζοντας τα κατάλληλα αντιμέτρα. Τελικά οι αναγνωρισμένες απαιτήσεις ασφαλείας καθώς και οι επιλεγμένοι χειρισμοί εισάγονται στη συνήθη διαδικασία λειτουργίας του συστήματος, ώστε να συμπεριληφθούν αποτελεσματικά στις

λειτουργικές απαιτήσεις του, καθώς και στις υπόλοιπες σχετικές απαιτήσεις. (π.χ. αξιοπιστία, δυνατότητα συντήρησης και υποστήριξης)[35].

Γενικά, η ασφάλεια σχετίζεται με σημαντικούς τομείς , όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Αυτοί οι παράγοντες γίνονται τελικά δομικά στοιχεία που χρησιμοποιούνται στο σχεδιασμό ασφαλών συστημάτων. Αυτοί οι σημαντικοί λοιπόν τομείς της ασφάλειας εφαρμόζονται στις τρεις κύριες κατηγορίες στοιχείων που πρέπει να ασφαλιστούν, δηλαδή στα δεδομένα, το λογισμικό και τις επιμέρους συσκευές που χρησιμοποιούνται. Η εκάστοτε υποδομή ενός συστήματος δημιουργεί μοναδικές προκλήσεις ασφαλείας που πρέπει να ληφθούν υπόψη αναλυτικά [36].

4.1.3 Ιδιωτικότητα και εμπιστευτικότητα

Η εμπιστευτικότητα αναφέρεται στο γεγονός πως μόνο εξουσιοδοτημένες ομάδες ή συστήματα μπορούν να αποκτήσουν πρόσβαση σε προστατευόμενα δεδομένα. Ο κίνδυνος της έκθεσης δεδομένων αυξάνεται σ ένα διευρυμένο σύστημα, λόγω του αυξημένου αριθμού των συμμετεχόντων, συσκευών και εφαρμογών που χρησιμοποιούνται, δηλαδή τελικά σε αύξηση των σημείων πρόσβασης στο σύστημα[37].

Η μεταβίβαση του ελέγχου των δεδομένων στο σύστημα οδηγεί σε μια αύξηση το κινδύνου έκθεσης των δεδομένων, καθώς αυτά καθίστανται προσβάσιμα σε διευρυμένο αριθμό μερών. Ανακύπτουν λοιπόν κάποιες ανησυχίες σχετικά με ζητήματα ασφάλειας των εφαρμογών, της ιδιωτικότητας, της κατοχής των δεδομένων από πολλές πλευρές αλλά και της ακεραιότητας τους[38][39].

Η εμπιστευτικότητα των δεδομένων στο σύστημα είναι άμεσα συνδεδεμένη με την ταυτοποίηση του εκάστοτε χρήστη. Η προστασία ενός λογαριασμού χρήστη από κλοπή είναι μία παράμετρος ενός μεγαλύτερου ζητήματος που αφορά τον έλεγχο πρόσβασης σε επιμέρους αντικείμενα, όπως η μνήμη, οι συσκευές, το λογισμικό κλπ. Η ηλεκτρονική ταυτοποίηση είναι η διαδικασία «εγκαθίδρυσης» εμπιστοσύνης στην ιδιότητα του χρήστη, όπως παρουσιάζεται αυτή ηλεκτρονικά σε ένα σύστημα πληροφορικής. Η έλλειψη ισχυρού ελέγχου της ταυτότητας ενός χρήστη, μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς χρηστών στο σύστημα, δημιουργώντας ένα κενό ασφαλείας[37].

Η *εμπιστευτικότητα του λογισμικού* είναι εξίσου σημαντική με αυτή των δεδομένων στη συνολική ασφάλεια του συστήματος. Η εμπιστευτικότητα του λογισμικού αναφέρεται στην ύπαρξη εμπιστοσύνης σε συγκεκριμένες εφαρμογές η διαδικασίες που θ διατηρούν και θα χειρίζονται τα προσωπικά δεδομένα με ασφαλή τρόπο. Οι εφαρμογές λογισμικού που αλληλοεπιδρούν με τα δεδομένα του χρήστη πρέπει να είναι πιστοποιημένες πως δεν θα εισάγουν επιπλέον κινδύνους που αφορούν την εμπιστευτικότητά και την ιδιωτικότητα. Ο κάτοχος του συστήματος είναι υπεύθυνος για να παρέχει ασφαλείς συνθήκες, οι οποίες ν βεβαιώνουν την ιδιωτικό ήτα του χρήστη[37][39][40].

Ως ιδιωτικότητα ορίζεται η επιθυμία ενός ατόμου να ελέγχει την αποκάλυψη των πληροφοριών του. Οι οργανισμοί που ασχολούνται με τα δεδομένα προσωπικού χαρακτήρα επιβάλλεται να υπακούν στο νομικό πλαίσιο της χώρας τους, το οποίο εξασφαλίζει κατάλληλα την ιδιωτικότητα και την εμπιστευτικότητα. Σε τέτοια συστήματα λοιπόν παρουσιάζονται νομικές προκλήσεις σε ζητήματα ασφαλείας που αφορούν την αποθήκευση δεδομένων σε πολλαπλές τοποθεσίες, συμβάλλοντας περαιτέρω στον κίνδυνο διαρροής τους[40].

4.1.4 Ακεραιότητα

Μια βασική πτυχή της ασφάλειας ενός πληροφοριακού συστήματος είναι η ακεραιότητα. Ακεραιότητα σημαίνει ότι τα στοιχεία του συστήματος μπορούν να τροποποιηθούν μόνο από εξουσιοδοτημένα μέλη και με εξουσιοδοτημένους τρόπους και αναφέρεται σε δεδομένα, λογισμικό και υλικό[41].

Η ακεραιότητα δεδομένων αναφέρεται στην προστασία των δεδομένων από μη εξουσιοδοτημένη διαγραφή, τροποποίηση ή πλαστογράφηση. Η διαχείριση της αποδοχής και των δικαιωμάτων μιας οντότητας σε συγκεκριμένους πόρους του συστήματος διαβεβαιώνει ότι πολύτιμα δεδομένα και υπηρεσίες δεν καταστρατηγούνται, δεν υπεξαιρούνται και δεν κλέπτονται. Αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση, ένας οργανισμός επιτυγχάνει μεγαλύτερη σιγουριά όσον αφορά την ακεραιότητα των δεδομένων και του συστήματος. Επιπλέον, τέτοιοι μηχανισμοί προσφέρουν τη μεγαλύτερη διαφάνεια αναφορικά με το ποιος ή τι μπορεί να έχει τροποποιήσει δεδομένα ή πληροφορίες του συστήματος, επηρεάζοντας ενδεχομένως την ακεραιότητα τους[42][43].

Η εξουσιοδότηση είναι ο μηχανισμός με τον οποίο ένα σύστημα καθορίζει το επίπεδο πρόσβασης που πρέπει να έχει ένας πιστοποιημένος χρήστης ώστε να διασφαλίζονται οι πόροι που ελέγχονται από αυτό. Λόγω του αυξανόμενου αριθμού των οντοτήτων και των σημείων πρόσβασης σ' ένα σύστημα όπως αυτό που εξετάζουμε, η εξουσιοδότηση είναι ένα ζωτικής σημασίας παράγοντας που διασφαλίζει πως μόνο εξουσιοδοτημένες οντότητες μπορούν να αλληλοεπιδράσουν με τα δεδομένα[44].

Η ακεραιότητα του λογισμικού αναφέρεται στην προστασία του λογισμικού από μη εξουσιοδοτημένη διαγραφή, τροποποίηση, κλοπή ή πλαστογράφηση. Τέτοιες πρακτικές μπορεί να συμβούν ηθελημένα ή ακούσια. Στο σύστημα επιχειρησιακής νοημοσύνης που μελετάμε η ευθύνη για την προστασία της ακεραιότητας του λογισμικού μεταφέρεται στον ιδιοκτήτη του λογισμικού και στον διαχειριστή του συστήματος[45].

4.1.5 Διαθεσιμότητα

Η διαθεσιμότητα αναφέρεται στη δυνατότητα των υπηρεσιών ενός συστήματος να είναι προσβάσιμες και να μπορούν να χρησιμοποιηθούν όποτε επιθυμεί ένας εξουσιοδοτημένος χρήστης. Ο administrator του συστήματος χρειάζεται να εγγυηθεί

πως οι πληροφορίες και η δυνατότητα επεξεργασίας τους είναι άμεσα διαθέσιμες στους χρήστες. Τέτοιου είδους συστήματα βασίζονται σε μεγάλο βαθμό στη διαθεσιμότητα των δομών και του δικτύου σε κάθε χρονική στιγμή[46].

Η κατανόηση και η ξεκάθαρη καταγραφή των συγκεκριμένων απαιτήσεων κάθε χρήστη είναι επιτακτική για το σχεδιασμό μιας λύσης που στοχεύει ακριβώς σε αυτές τις ανάγκες. Η επιβεβαίωση της ιδιότητας των χρηστών, που σε πολλές περιπτώσεις μοιράζονται κοινές βασικές απαιτήσεις ασφαλείας και ο καθορισμός συγκεκριμένων αναγκών για την προστασία των δεδομένων και των πληροφοριών μπορεί να είναι ένα από τα πιο σύνθετα ζητήματα στο σχεδιασμό ενός συστήματος πληροφορικής. Αυτό το πολυχρηστικό, διαμοιρασμένο περιβάλλον προτάσσει μοναδικά ζητήματα ασφαλείας, τα οποία βασίζονται στο επίπεδο ο χρήστης επιχειρεί, τόσο σε φυσική, όσο και σε εικονική παρουσία[47].

4.2 Ιδιωτικότητα στην υγεία και ασφάλεια στις Ηλεκτρονικές Υπηρεσίες Υγείας

Οι ηλεκτρονικές υπηρεσίες υγείας χρησιμοποιούνται όλο και περισσότερο από ασθενείς, γιατρούς και άλλους εργαζόμενους στον τομέα της υγείας. Οι υπηρεσίες αυτές έχουν σημαντικά πλεονεκτήματα , όπως τη μείωση του κόστους των υπηρεσιών παροχής υγείας και την παροχή πιο γρήγορης και πιο αποτελεσματικής επεξεργασίας των δεδομένων. Ωστόσο, η χρήση των ηλεκτρονικών υπηρεσιών υγείας αυξάνει τις ανησυχίες για την ασφάλεια, την ακεραιότητα και την ιδιωτικότητα των προσωπικών ιατρικών δεδομένων. Τέτοιες ανησυχίες επηρεάζουν τη θέληση των ασθενών στο να αποκαλύψουν τα ιατρικά τους στοιχεία και μπορεί να προκαλέσουν συνέπειες που επηρεάζουν την υγεία τους, ή ακόμα και τη ζωή τους[48].

Μια μη εξουσιοδοτημένη έκθεση πληροφοριών για την υγεία ενός ατόμου μπορεί να δημιουργήσει αρκετά προβλήματα στο άτομο αυτό. Τέτοια προβλήματα μπορεί να είναι η απόρριψη τους από μία πιθανή ευκαιρία απασχόλησης, η δυσκολία στην απόκτηση ή συνέχιση ενός ασφαλιστικού συμβολαίου ή δανείου, ο κοινωνικός αποκλεισμός, η απομόνωση του από τα υπόλοιπα μέλη της οικογένειας του αλλά και το αίσθημα ντροπής που ενδεχομένως να νιώσει. Η ζημιά που μπορεί να προκαλέσει μια διαρροή προσωπικών δεδομένων δεν μπορεί να διορθωθεί. Για αυτό το λόγο, είναι ζωτικής σημασίας να προληφθεί μια τέτοια διαρροή και όχι απλά να ανιχνευθεί εκ των υστέρων μέσω διαδικασιών ελέγχου, ώστε να μπορεί να κερδηθεί η εμπιστοσύνη του κοινού που θα τις χρησιμοποιήσει[49].

Η ευρεία υποστήριξη των καταναλωτών για ηλεκτρονικά αρχεία υγείας βασίζεται στη δικαιολογημένη και καλώς δομημένη εμπιστοσύνη ότι το σύστημα θα προστατεύσει τις εξαιρετικά ευαίσθητες πληροφορίες για την υγεία τους σύμφωνα με τη συγκατάθεση που επιβάλλεται να δώσουν ή να παρακρατήσουν. Αυτό περιλαμβάνει την κάλυψη των αναγκών των καταναλωτών με ιδιαίτερα απαιτητικές ανάγκες απορρήτου, όπως τα άτομα που λαμβάνουν θεραπεία για ευαίσθητες ασθένειες (HIV/AIDS, εθισμός, ψυχιατρικές ασθένειες κ.λπ.), επαγγελματίες υγείας που λαμβάνουν θεραπεία και διασημότητες.

Εάν οι ηλεκτρονικές υπηρεσίες υγείας πρόκειται να υιοθετηθούν και να υποστηριχθούν από τους καταναλωτές, οι ανησυχίες για την προστασία της ιδιωτικής τους ζωής πρέπει να αντιμετωπιστούν[50].

4.3 Γενικές κατηγορίες στις Ηλεκτρονικές Υπηρεσίες Υγείας

4.3.1 Αρχιτεκτονική

Η αρχιτεκτονική είναι ένα από τα σημαντικότερα ζητήματα που προκύπτει κατά το σχεδιασμό μιας προτεινόμενης υπηρεσίας υγειονομικής περίθαλψης. Δεδομένου ότι τα δεδομένα υγείας των ασθενών διανέμονται σε πολλές οντότητες, όπως νοσοκομεία, κέντρα υγειονομικής περίθαλψης και άλλα απομακρυσμένα συστήματα, οι συγκεντρωτικές λύσεις δεν θα ήταν βολικές[48].

4.3.2 Έλεγχος πρόσβασης

Κατά το διαμοιρασμό των πληροφοριών βάσει συναίνεσης, οι ίδιοι οι ασθενείς είναι σε θέση να καθορίσουν τις πολιτικές που ελέγχουν την πρόσβαση τρίτων σε προσωπικές πληροφορίες όσον αφορά την υγεία τους. Το γεγονός αυτό καταδεικνύει μια σημαντική απόκλιση από την παραδοσιακή προσέγγιση όπου οι οργανισμοί υγείας καθιέρωναν την πολιτική πρόσβασης σε αυτές τις πληροφορίες.[51] Η αλλαγή αυτή είναι απαραίτητη, διότι οι οργανισμοί υγειονομικής περίθαλψης διασυνδέουν πλέον τα συστήματά τους ώστε να παρέχουν καλύτερες υπηρεσίες, αυξάνοντας τις δυνατότητες μη εξουσιοδοτημένης πρόσβασης.

Δεδομένου ότι υπάρχει μια πληθώρα μεμονωμένων σεναρίων, περιστάσεων και σχέσεων, το πλαίσιο ελέγχου πρόσβασης πρέπει να είναι ευέλικτο και σωστά εκφρασμένο ώστε να διασφαλίζεται ότι η πολιτική πρόσβασης του ασθενούς μπορεί να καταγράφεται και να εφαρμόζεται με τρόπο που να αντικατοπτρίζει την κατανόησή τους όσον αφορά την επιθυμία τους για το ποιος θέλουν να έχουν πρόσβαση και ποιος δεν θέλουν να έχει πρόσβαση[52].

4.3.3 Καταστάσεις έκτακτης ανάγκης

Τα χαρακτηριστικά έκτακτης ανάγκης που απαντώνται σε μια ηλεκτρονική υπηρεσία υγείας επικεντρώνονται στις εξαιρέσεις όπου χρειάζεται να παρακαμφθεί η συγκατάθεση των ασθενών. Τέτοιες δράσεις χρειάζονται όταν ο ασθενής δεν είναι σε θέση να ελέγξει τα δεδομένα υγείας του. Σε μια κατάσταση έκτακτης ανάγκης, πρέπει να γίνουν νομικές ενέργειες, να προστατευθεί η προστασία της ιδιωτικότητας και οι εξαιρέσεις να αποφασίζονται με μια λεπτή προσέγγιση[46].

4.3.4 Ανωνυμία

Είναι απαραίτητο να χρησιμοποιηθούν συγκεκριμένες μέθοδοι που εξασφαλίζουν την ανωνυμία σε μια ηλεκτρονική υπηρεσία υγείας, ώστε να διατηρηθούν μυστικά

τα ευαίσθητα προσωπικά δεδομένα του ασθενούς αλλά και η ταυτότητα του από μη εξουσιοδοτημένους τρίτους[43].

4.4 Ζητήματα ασφαλείας στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης

Τα ζητήματα ασφαλείας που πρέπει να διευθετηθούν στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης είναι:

- Η διασφάλιση της διαθεσιμότητας των πληροφοριών που μεταδίδονται ή αποθηκεύονται μεταξύ των συμμετεχόντων οντοτήτων.
- Η διατήρηση της ακεραιότητας των πληροφοριών που μεταδίδονται μεταξύ των συμμετεχόντων συστημάτων ή που αποθηκεύονται εντός των συμμετεχόντων μερών, δηλαδή να αποτρέπεται η απώλεια ή η τροποποίηση των πληροφοριών λόγω μη εξουσιοδοτημένης πρόσβασης, βλάβης σε κάποιο κομμάτι του συστήματος ή άλλων σφαλμάτων.[53]
- Η διατήρηση της ακεραιότητας των παρεχόμενων υπηρεσιών, δηλαδή η εμπιστευτικότητα και η σωστή λειτουργία του συστήματος.
- Η παροχή ελέγχου της πρόσβασης στις υπηρεσίες ή τα στοιχεία τους, ώστε να εξασφαλίζεται ότι οι χρήστες μπορούν να χρησιμοποιούν μόνο τις υπηρεσίες για τις οποίες έχουν εξουσιοδοτηθεί.
- Η εξακρίβωση της ταυτότητας των επικοινωνούντων εταίρων.
- Όπου είναι απαραίτητη, η παροχή ασφαλούς συνεργασίας με πιο ανοιχτά εξωτερικά συστήματα[54].

- Επιπρόσθετα, χρειάζεται:

- Να διασφαλιστεί η εμπιστευτικότητα των πληροφοριών που διατηρούνται μέσα στο σύστημα.
- Να γίνει σαφής διαχωρισμός δεδομένων και διαδικασιών στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης, εξασφαλίζοντας διαρροή μηδενικών δεδομένων μεταξύ διαφορετικών εφαρμογών.
- Να διατηρείται το ίδιο επίπεδο ασφαλείας κατά την προσθήκη ή την αφαίρεση πόρων σε φυσικό επίπεδο[55].

4.5 Μηχανισμοί και τεχνικές που χρησιμοποιούνται στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης

Για να επιλεγούν οι κατάλληλοι μηχανισμοί και τεχνικές που επιτρέπουν στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης θα πρέπει να εξεταστούν τα επιμέρους μέρη του, ούτως ώστε η επικοινωνία μεταξύ τους να είναι εναρμονισμένη με τα ζητήματα που τέθηκαν παρακάτω. Η δημιουργία λοιπόν ενός τέτοιου ασφαλούς συστήματος παρουσιάζεται σε αυτή την ενότητα, με τη σειρά που αναφέρθηκε παραπάνω, ξεκινώντας από την αρχιτεκτονική του δικτύου και τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται, συνεχίζεται με τον έλεγχο πρόσβασης των χρηστών στο σύστημα

και την πρόβλεψη μιας κατάστασης έκτακτης ανάγκης και τελειώνει με την διασφάλιση της ανωνυμίας κατά τη διάρκεια της χρήσης του[31][48].

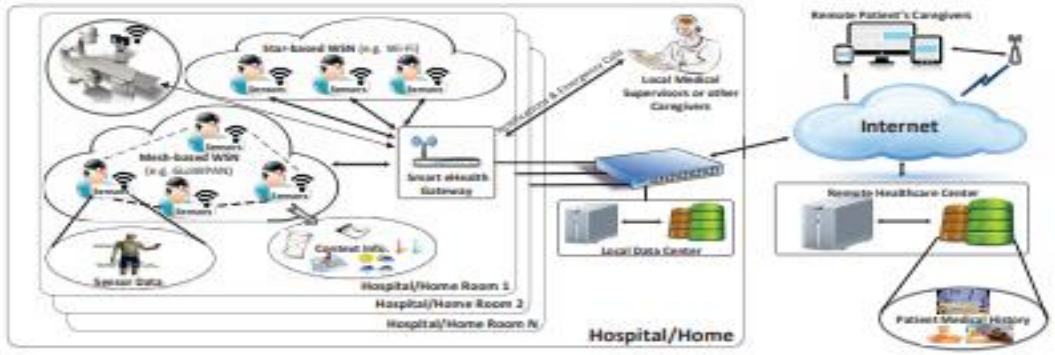
4.5.1 Αρχιτεκτονική του Δικτύου και πρωτόκολλα κρυπτογράφησης των επικοινωνιών

Η αρχιτεκτονική του δικτύου του ιατρικής επιχειρησιακής νοημοσύνης περιλαμβάνει τα ακόλουθα κύρια μέρη:

Δίκτυο ιατρικών αισθητήρων: Το πρώτο μέρος του συστήματος, το οποίο είναι και αυτό που έρχεται σε επαφή ο εκάστοτε ασθενής είναι το δίκτυο των ιατρικών αισθητήρων, όπως έχει αναλυθεί σε προηγούμενο κεφάλαιο. Οι αισθητήρες αυτοί συλλέγουν ιατρικές και άλλες μετρήσεις από το σώμα και το δωμάτιο που χρησιμοποιείται για τη χρήση του συστήματος, ώστε να μπορεί να πραγματοποιηθεί η διάγνωση και η αξιολόγηση της ιατρικής κατάστασης του ασθενούς.[56] Τα σήματα των αισθητήρων στη συνέχεια μεταδίδονται στην πύλη μέσω ασύρματων ή ενσύρματων πρωτοκόλλων επικοινωνίας όπως Serial, SPI, Bluetooth, Wi-Fi ή IEEE 802.15.4. [57]

Έξυπνη πύλη: Η πύλη αυτή υποστηρίζει διαφορετικά πρωτόκολλα επικοινωνίας και ενεργεί ως το σημείο επαφής μεταξύ του δικτύου των αισθητήρων και του τοπικού υπολογιστικού συστήματος. Λαμβάνει δεδομένα από διαφορετικά υποδίκτυα, πραγματοποιεί μετατροπές πρωτοκόλλου και παρέχει υπηρεσίες υψηλότερου επιπέδου, όπως τη συγκέντρωση των δεδομένων, το φιλτράρισμα και μείωση των διαστάσεων τους[58].

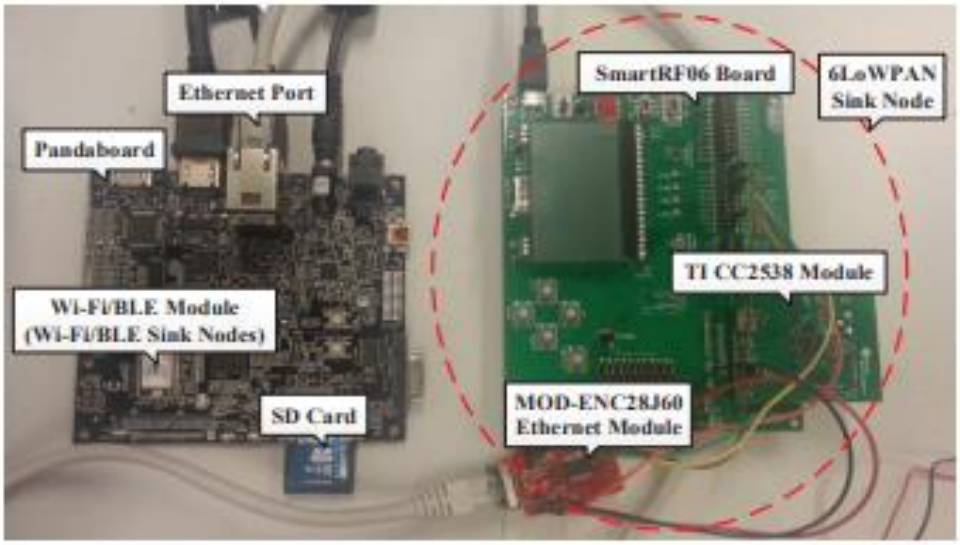
Back-end σύστημα: Το πίσω μέρος του συστήματος αποτελείται από τα δύο υπόλοιπα στοιχεία, δηλαδή ένα τοπικό switch και μια πλατφόρμα υπολογιστικού συστήματος που περιλαμβάνει την αποστολή δεδομένων και το αναλυτικό λογισμικό, τους διακομιστές και τελικά τους υπολογιστές-πελάτες.



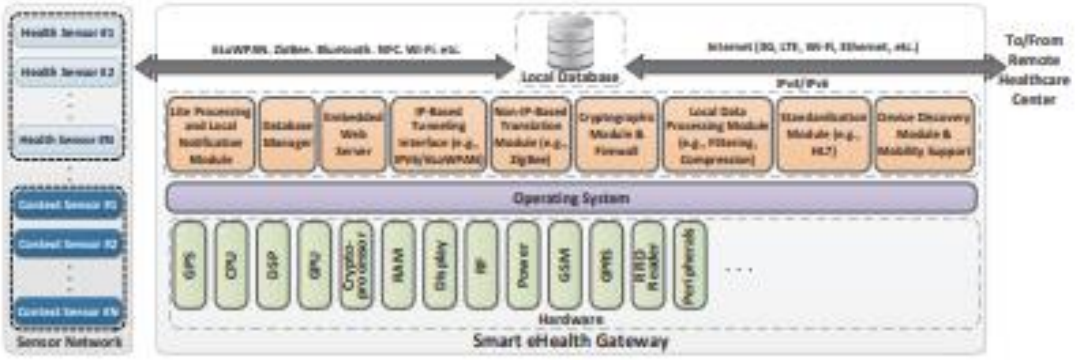
Εικόνα 2: Η αρχιτεκτονική του δικτύου του συστήματος MBI[58]

Όπως μπορεί να παρατηρηθεί από το σχήμα, η στρατηγική θέση της έξυπνης πύλης μπορεί να αξιοποιηθεί, ώστε να προσφέρει πολλές υπηρεσίες υψηλότερου επιπέδου για την ενίσχυση των χαρακτηριστικών του συστήματος σε πολλές διαφορετικές πτυχές. Ο βασικός λόγος χρήσης μιας τέτοιας πύλης στην ηλεκτρονική υγεία είναι η

υποστήριξη διαφόρων ασύρματων πρωτοκόλλων και επικοινωνίας μεταξύ συσκευών.



Εικόνα 3: Υλοποίηση της έξυπνης πύλης[58]



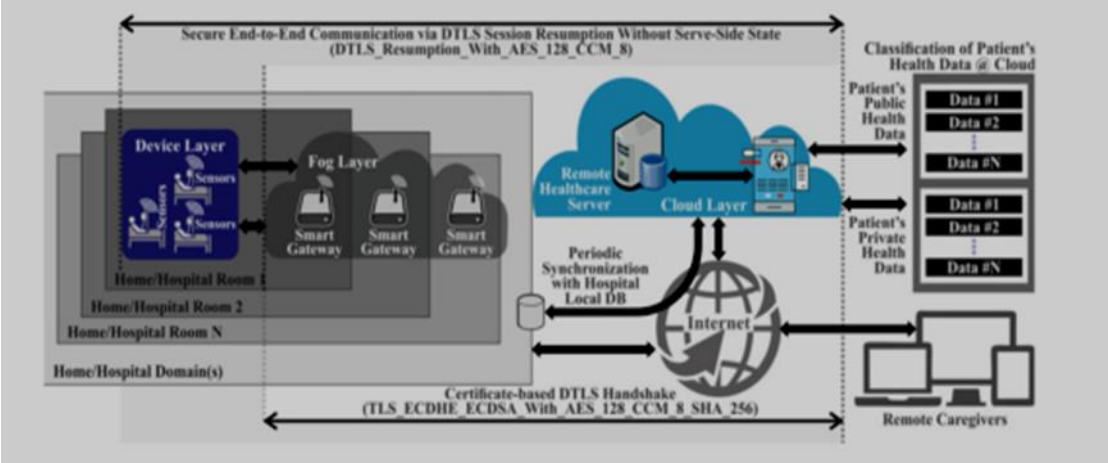
Εικόνα 4 Αρχιτεκτονική της έξυπνης πύλης[58]

Η προτεινόμενη αρχιτεκτονική μας εκμεταλλεύεται το ρόλο των έξυπνων πυλών στο στρώμα ομίχλης (fog layer) για την ασφαλή και αποτελεσματική πιστοποίηση και εξουσιοδότηση απομακρυσμένων τελικών χρηστών για λογαριασμό των αισθητήρων και των υπόλοιπων συσκευών επικοινωνίας που χρησιμοποιούνται στο σύστημα. Παρέχοντας το καθιερωμένο πλαίσιο σύνδεσης στους κόμβους των ιατρικών αισθητήρων, οι συσκευές αυτές δεν χρειάζεται πλέον να πιστοποιούν την ταυτότητα και να εξουσιοδοτούν ένα απομακρυσμένο κέντρο υγείας ή έναν φροντιστή. Έτσι, οποιαδήποτε κακόβουλη δραστηριότητα μπορεί να αποκλειστεί πριν εισέλθει σε έναν περιορισμένο ιατρικό τομέα[59].

Σε μια τέτοια αρχιτεκτονική, οι πληροφορίες που σχετίζονται με την υγεία των ασθενών καταγράφονται από αισθητήρες που φοριούνται στο σώμα ή εμφυτεύονται, με τους οποίους ο ασθενής είναι εξοπλισμένος για την προσωπική

παρακολούθηση πολλαπλών παραμέτρων. Αυτά τα δεδομένα υγείας μπορούν επίσης να συμπληρωθούν με πληροφορίες περιβάλλοντος (π.χ. ημερομηνία, ώρα, τοποθεσία και θερμοκρασία) που επιτρέπουν τον εντοπισμό ασυνήθιστων μορφών και την ακριβέστερη εξαγωγή συμπερασμάτων σχετικά με την κατάσταση.[59][60]

Η προτεινόμενη αρχιτεκτονική του δικτύου λοιπόν επικεντρώνεται στο γεγονός ότι η έξυπνη πύλη ηλεκτρονικής υγείας και ο απομακρυσμένος τελικός χρήστης διαθέτουν επαρκείς πόρους για την εκτέλεση διαφόρων πρωτοκόλλων ασφαλείας καθώς και την επικύρωση πιστοποιητικών. Για την παροχή επικοινωνίας από άκρο σε άκρο μεταξύ ενός απομακρυσμένου τελικού χρήστη και μιας απομακρυσμένης ιατρικής συσκευής, εισάγονται έξυπνες πύλες ηλεκτρονικής υγείας για την κατασκευή ενός πρωτοκόλλου ασφαλείας μεταφορικού στρώματος το οποίο είναι το Datagram Transport Layer Security (DTLS)[60].



Εικόνα 5: Επισκόπηση της επικοινωνίας των μερών του συστήματος MBI[60]

4.5.1.1 Χειραψία DTLS

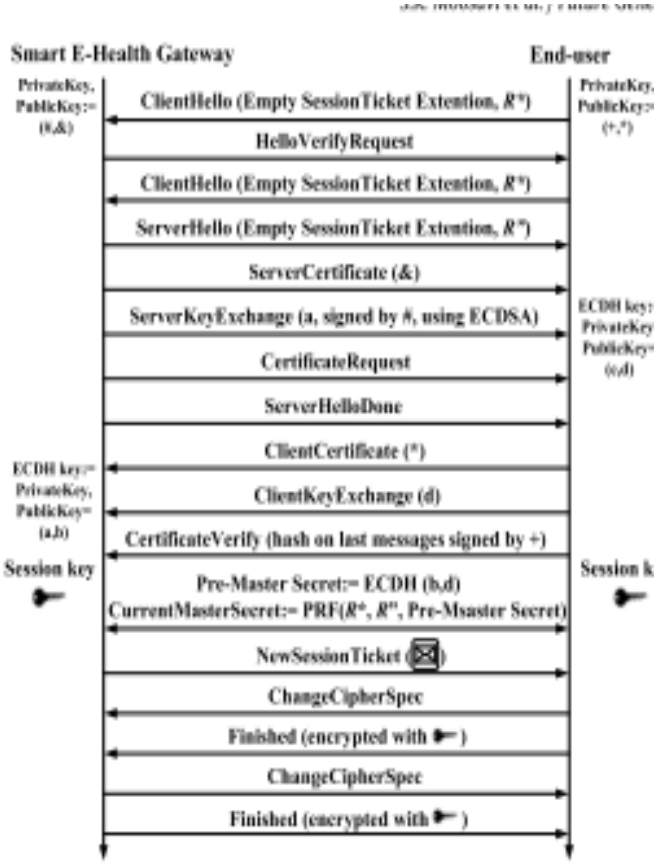
Το πρωτόκολλο χειραψίας DTLS αποτελεί τη βασική λύση ασφάλειας για το επίπεδο μεταφοράς. Μια πλήρης χειραψία ξεκινά με ένα μήνυμα ClientHello, το οποίο περιλαμβάνει τις παραμέτρους ασφαλείας για τη σύνδεση που χρησιμοποιείται αργότερα κατά τη διάρκεια της χειραψίας για τον υπολογισμό του πριν το κύριο μυστικού κλειδιού.

Το πρώτο πιστοποιητικό στην αλυσίδα περιλαμβάνει το δημόσιο κλειδί της έξυπνης πύλης που δημιουργείται με το OpenSSL στην έκδοση 1.0.1.j. Το OpenSSL είναι ένα έργο ανοιχτού κώδικα για την υλοποίηση SSL, TLS και διάφορων βιβλιοθηκών κρυπτογραφίας όπως είναι το συμμετρικό κλειδί, το δημόσιο κλειδί και οι αλγόριθμοι κατακερματισμού. Χρησιμοποιείται συνήθως για τη δημιουργία και τη διαχείριση κλειδιών και πιστοποιητικών. Μόλις επικυρωθεί το πιστοποιητικό, ο τελικός χρήστης μπορεί να εξάγει το δημόσιο κλειδί της έξυπνης πύλης.

Το μήνυμα CertificateRequest αποστέλλεται μόνο σε αμοιβαία χειραψία και περιλαμβάνει τις λίστες των έγκυρων πιστοποιητικών της έξυπνης πύλης. Το μήνυμα

ServerKeyExchange αποστέλλεται μόνο με συγκεκριμένες σουίτες κρυπτογράφησης που χρειάζονται περισσότερες παραμέτρους για τον υπολογισμό ενός κύριου μυστικού κλειδιού[61].Η σουίτα κρυπτογράφησης που χρησιμοποιείται σε αυτή την εργασία είναι TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8_SHA_256. Το όνομα δηλώνει τη χρήση της ελλειπτικής κρυπτογραφίας, ιδιαίτερα της Ελλειπτικής Καμπύλης Diffie-Hellman (Elliptic Curve Diffie-Hellman ECDH) και του αλγόριθμου ψηφιακής υπογραφής ελλειπτικής καμπύλης (Elliptic Curve Digital Signature Algorithm (ECDSA).

Επιπλέον, για την κρυπτογράφηση χρησιμοποιείται AES-based CCM με 4 από 8 bytes. Με αυτήν τη σουίτα κρυπτογράφησης, το μήνυμα ServerKeyExchange περιέχει το δημόσιο κλειδί ECDH της έξυπνης πύλης και τις λεπτομέρειες της σχετικής ελλειπτικής καμπύλης. Οι αλγόριθμοι αυτοί για την κρυπτογράφηση αναλύονται λίγο παρακάτω[62].



Εικόνα 6: Η χειραψία DTLS[60]

Το ClientKeyExchange περιλαμβάνει πρόσθετες παραμέτρους που χρησιμοποιούνται για τον υπολογισμό του κύριου μυστικού κλειδιού. Σε αυτήν την περίπτωση μεταδίδεται το δημόσιο κλειδί ECDH της έξυπνης πύλης. Το CertificateVerify είναι ένα μήνυμα που επιτρέπει στον τελικό χρήστη να αποδείξει στην έξυπνη πύλη ότι κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιέχεται στο πιστοποιητικό. Έτσι, μεταδίδεται μόνο στον αμοιβαίο έλεγχο ταυτότητας.

Με το μήνυμα ChangeCipherSpec, ο τελικός χρήστης ενημερώνει την έξυπνη πύλη ότι τα επόμενα μηνύματα θα κρυπτογραφηθούν χρησιμοποιώντας τις συμφωνημένες σουίτες κρυφών κωδικών και μυστικά κλειδιά.

Το μήνυμα "Finished" περιλαμβάνει την κρυπτογραφημένη κατακερματισμό πάνω από όλα τα μηνύματα πτήσης (flight messages) που εξασφαλίζουν ότι και οι δύο επικοινωνούντες πλευρές πραγματοποιούν χειραψία βάσει μη τροποποιημένων μηνυμάτων πτήσης και η χειραψία εκτελείται με επιτυχία. Με τα μηνύματα "Finished", οι δύο πλευρές συμφωνούν να στέλνουν και να λαμβάνουν ασφαλώς προστατευμένες πληροφορίες εφαρμογής μέσω αυτής της σύνδεσης.

Υποτίθεται ότι στο πλαίσιο της χειραψίας DTLS με βάση τα πιστοποιητικά, από την μία πλευρά, η έξυπνη πύλη πιστοποιεί (Authreq.1) τον απομακρυσμένο τελικό χρήστη μέσω πιστοποιητικών. Από αυτή την άποψη, παρόμοια με τα τρέχοντα προγράμματα περιήγησης ιστού, οι έξυπνες πύλες διαθέτουν μια ομάδα αξιόπιστων πιστοποιητικών. Από την άλλη πλευρά, η έξυπνη πύλη είτε πιστοποιεί (Auth-req.2) στον απομακρυσμένο τελικό χρήστη μέσω πιστοποιήσεων κατά τη χειραψία DTLS είτε με βάση έναν κωδικό πρόσβασης σε επίπεδο εφαρμογής μόλις τερματιστεί η χειραψία.

Μόλις ολοκληρωθεί με επιτυχία ο αμοιβαίος έλεγχος ταυτότητας μεταξύ του τελικού χρήστη και της έξυπνης πύλης, ο τελικός χρήστης εξουσιοδοτεί (Authz.) ως αξιόπιστη οντότητα, έτσι ώστε ένα ερώτημα δεδομένων από την πλευρά των τελικών χρηστών να μεταδοθεί στον ιατρικό αισθητήρα μέσω του έξυπνη πύλη. Για να διευκολυνθεί η ασφάλεια και η εξουσιοδότηση της επικοινωνίας, απαιτείται και οι δύο οντότητες, ο περιορισμένος ιατρικός αισθητήρας και η έξυπνη πύλη να εξουσιοδοτούν ο ένας τον άλλο ταυτόχρονα (Mut-auth.) κατά τη διάρκεια της φάσης αρχικοποίησης.

Αυτό γίνεται με εκτέλεση χειραψίας DTLS με βάση το δημόσιο κλειδί και μεταξύ των δύο οντοτήτων. Αν και η συμμετρική χειραψία DTLS βασισμένη στο κλειδί παρέχει μια αποτελεσματική εναλλακτική λύση για τη χειραψία DTLS με βάση το δημόσιο κλειδί, η συμμετρική χειραψία βασισμένη στο κλειδί χρειάζεται μυστικά κλειδιά για να διανεμηθεί και να είναι άμεσα διαθέσιμη και στα δύο τελικά σημεία της επικοινωνίας. Επιπλέον, σε σύγκριση με τη συμμετρική χειραψία DTLS με βάση το κλειδί, η απόκτηση μυστικών σημείων σε μια χειραψία με βάση το δημόσιο κλειδί συνεπάγεται τον υπολογισμό του προβλήματος διακριτού λογαρίθμου ελλειπτικής καμπύλης. Δεδομένου ότι η επίλυση του προβλήματος διακριτού λογαρίθμου είναι εξίσου δύσκολη με την παραγοντοποίηση ακέραιων αριθμών, το πρόβλημα αυτό δεν μπορεί να λυθεί χωρίς κόπο[63][61][64].

Μόλις ολοκληρωθεί η αμοιβαία επαλήθευση ταυτότητας και η ανταλλαγή κλειδιών του πρωτοκόλλου, οι δύο επικοινωνούντες απαιτείται να συμφωνήσουν σε ένα κοινό κλειδί. Αυτό το κοινό κλειδί μπορεί να δημιουργηθεί χρησιμοποιώντας μια ήδη συμφωνημένη ελλειπτική καμπύλη μεταξύ των δύο συνομηλίκων. Χρησιμοποιώντας την κοινοποιημένο κοινό κλειδί, ο ένας συνομιλητής (για παράδειγμα ένας περιορισμένος ιατρικός αισθητήρας) κρυπτογραφεί το συγκεντρωμένα ιατρικά

δεδομένα των ασθενών εφαρμόζοντας το αποτελεσματικό πρότυπο Advanced Encryption Standard (AES-CCM) και μεταδίδει τις κρυπτογραφημένες ιατρικές πληροφορίες (Enc./Dec.) στην έξυπνη πύλη ηλεκτρονικής υγείας και αντίστροφα[62].

4.5.1.2 Ελλειπτική καμπύλη Diffie-Hellman

Η ελλειπτική καμπύλη Diffie-Hellman (ECDH) είναι ένα ανώνυμο πρωτόκολλο συμφωνίας κλειδιού που επιτρέπει σε δύο μέρη, καθένα από τα οποία έχει ένα ζεύγος κλειδιών δημόσιου και ιδιωτικού κλειδιού ελλειπτικής καμπύλης, να δημιουργήσει ένα κοινό μυστικό πάνω σε ένα ανασφαλές κανάλι. Αυτό το κοινόχρηστο μυστικό μπορεί να χρησιμοποιηθεί άμεσα ως κλειδί ή για να αντλήσει άλλο κλειδί. Το κλειδί ή το παράγωγο κλειδί μπορούν στη συνέχεια να χρησιμοποιηθούν για την κρυπτογράφηση μεταγενέστερων επικοινωνιών χρησιμοποιώντας έναν κρυπτογράφο συμμετρικού κλειδιού. Είναι μια παραλλαγή του πρωτοκόλλου Diffie-Hellman που χρησιμοποιεί κρυπτογράφηση ελλειπτικής καμπύλης[65].

Το παρακάτω παράδειγμα θα απεικονίσει τον τρόπο με τον οποίο γίνεται μια συμφωνία κλειδιού. Ας υποθέσουμε ότι ένας χρήστης θέλει να δημιουργήσει ένα κοινόχρηστο κλειδί με έναν άλλον χρήστη, αλλά το μόνο διαθέσιμο για αυτούς κανάλι μπορεί να παρακολουθείται από ένα τρίτο μέρος. Αρχικά, συμφωνούνται οι παράμετροι τομέα $((p, a, b, G, n, h)$ για την πρώτη περίπτωση, ή $(m, f(x), a, b, G, n, h))$ για τη δυαδική περίπτωση. Επίσης, κάθε μέρος πρέπει ν έχει ένα ζεύγος κλειδιών κατάλληλο για την κρυπτογραφία ελλειπτικής καμπύλης, το οποίο αποτελείται από ένα ιδιωτικό κλειδί d, το οποίο είναι ένας τυχαίος ακέραιος στο διάστημα $[1, n-1]$, και ένα δημόσιο κλειδί που αναπαρίσταται από ένα σημείο $Q = dG$.

Για να εκτελεστεί το πρωτόκολλο, κάθε χρήστης πρέπει να γνωρίζει το δημόσιο κλειδί του άλλου. Οπότε, εάν τα αντίστοιχα ζεύγη είναι(d_A, Q_A) και (d_B, Q_B) , ο πρώτος χρήστης υπολογίζει το σημείο $(x_k, y_k) = d_A Q_B$ και ο δεύτερος υπολογίζει το σημείο $(x_k, y_k) = d_B Q_A$. Το μοιραζόμενο μυστικό είναι το x_k, η συντεταγμένη x δηλαδή του σημείου. Τα περισσότερα πρωτόκολλα που βασίζονται σε ECDH παράγουν ένα συμμετρικό κλειδί από το x_k, χρησιμοποιώντας κάποια συνάρτηση παραγωγής κλειδιού.

Το κοινό μυστικό που υπολογίζουν και οι δύο μεριές είναι ίδιο καθώς $d_A Q_B = d_A d_b G = d_B d_A G = d_B Q_A$

Η μόνη πληροφορία σχετικά με το ιδιωτικό κλειδί του αρχικού χρήστη, που εκτίθεται αρχικά, είναι το δημόσιο κλειδί του. Έτσι, κανένα άλλο μέρος εκτός από αυτόν δεν μπορεί να καθορίσει το ιδιωτικό κλειδί του αρχικού χρήστη, εκτός αν το συμβαλλόμενο μέρος μπορεί να λύσει το πρόβλημα διακριτού λογαρίθμου της ελλειπτικής καμπύλης. Το ιδιωτικό κλειδί του δεύτερου χρήστη είναι εξίσου ασφαλές. Κανένα άλλο μέρος εκτός από τους δύο χρήστες δεν μπορεί να υπολογίσει το κοινό

μυστικό, εκτός αν το κάποιος τρίτος μπορεί να λύσει την ελλειπτική καμπύλη του προβλήματος Diffie-Hellman.

Τα δημόσια κλειδιά είναι είτε στατικά (και αξιόπιστα, π.χ. μέσω πιστοποιητικού) είτε εφήμερα (επίσης γνωστά ως ECDHE, όπου το τελικό «E» σημαίνει «εφήμερο»). Τα εφήμερα κλειδιά είναι προσωρινά και όχι απαραίτητα επικυρωμένα, οπότε αν είναι επιθυμητή η εξακρίβωση της γνησιότητας, πρέπει να λαμβάνονται διαβεβαιώσεις γνησιότητας με άλλα μέσα. Ο έλεγχος ταυτότητας είναι απαραίτητος για την αποφυγή προσβολών από άνθρωπο στη μέση. Εάν ένα από τα δημόσια κλειδιά των χρηστών είναι στατικό, τότε οι επιθέσεις man-in-the-middle (κοινή παραβίαση ασφάλειας, όπου ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους) αποτρέπονται. Τα στατικά δημόσια κλειδιά δεν προσφέρουν ούτε μυστικότητσ ούτε πλαστοπροσωπία εικονικής αντίστασης, μεταξύ άλλων προηγμένων χαρακτηριστικών ασφαλείας, οπότε οι κάτοχοι στατικών ιδιωτικών κλειδιών θα πρέπει να επικυρώσουν το άλλο δημόσιο κλειδί και θα πρέπει να εφαρμόσουν μια ασφαλή λειτουργία εξαγωγής κλειδιών στο κοινόχρηστο μυστικό Diffie-Hellman για να αποφύγουν τη διαρροή πληροφοριών σχετικά με το στατικό ιδιωτικό κλειδί.

Ενώ το κοινό μυστικό μπορεί να χρησιμοποιηθεί άμεσα ως κλειδί, είναι συχνά επιθυμητό να έχουμε το μυστικό για να αφαιρέσουμε τα αδύνατα κομμάτια λόγω της ανταλλαγής Diffie-Hellman[66].

4.5.1.3 Ελλειπτική Καμπύλη Αλγορίθμου Ψηφιακής Υπογραφής

Στην κρυπτογραφία, ο αλγόριθμος ψηφιακής υπογραφής ελλειπτικής καμπύλης (ECDSA) προσφέρει μια παραλλαγή του αλγορίθμου ψηφιακής υπογραφής (DSA) που χρησιμοποιεί κρυπτογράφηση ελλειπτικής καμπύλης.

Όπως συμβαίνει με την κρυπτογραφία ελλειπτικής καμπύλης γενικά, το μέγεθος bit του δημόσιου κλειδιού που πιστεύεται ότι είναι απαραίτητο για το ECDSA είναι περίπου διπλάσιο από το μέγεθος του επιπέδου ασφαλείας. Για παράδειγμα, σε ένα επίπεδο ασφάλειας 80 bit (που σημαίνει ότι ένας εισβολέας απαιτεί ενέργεια περίπου 2^{80} ενέργειες για να βρει το ιδιωτικό κλειδί) το μέγεθος ενός δημόσιου κλειδιού ECDSA θα είναι 160 bit, ενώ το μέγεθος ενός δημόσιου κλειδιού DSA είναι τουλάχιστον 1024 bits. Από την άλλη πλευρά, το μέγεθος υπογραφής είναι το ίδιο και για τα DSA και ECDSA: περίπου $4t$bits, όπου t είναι το επίπεδο ασφαλείας που μετράται σε bits, δηλαδή περίπου 320 bits για ασφάλεια επίπεδου 80 bits[67][68].

4.5.1.4 Πρότυπο Προηγμένης Κρυπτογράφησης

Το Πρότυπο Προηγμένης Κρυπτογράφησης (AES), αρχικά γνωστό ως Rijndael, είναι ένας αλγόριθμος κρυπτογράφησης συμμετρικού κλειδιού και το κυβερνητικό πρότυπο των ΗΠΑ για ασφαλή και ταξινομημένη κρυπτογράφηση και αποκρυπτογράφηση δεδομένων.

Το Δεκέμβριο του 2001, το Εθνικό Ινστιτούτο Προτύπων των ΗΠΑ (NIST) ενέκρινε το AES ως Πρότυπο Επεξεργασίας και Δημοσίευσης Ομοσπονδιακών Πληροφοριών (FIPS PUB), το οποίο καθορίζει την εφαρμογή του αλγορίθμου Rijndael σε όλα τα ευαίσθητα ταξινομημένα δεδομένα.[69]

Το AES διαθέτει τρία σταθερά κρυπτογράφους μπλοκ 128 bit με κρυπτογραφικά κλειδιά μεγέθους 128, 192 και 256 bits. Το μέγεθος κλειδιού είναι απεριόριστο, ενώ το μέγιστο μέγεθος μπλοκ είναι 256 bits. Ο σχεδιασμός του AES βασίζεται σε ένα δίκτυο υποκατάστασης μετασχηματισμού (Substitution Permutation Network SPN) και δεν χρησιμοποιεί το Data Encryption Standard (DES)[70].

Το 1997, η NIST ξεκίνησε μια διεργασία ανάπτυξης αλγορίθμων πέντε ετών για να αντικαταστήσει το DES και το Triple DES. Η διαδικασία επιλογής αλγορίθμου από το NIST διευκόλυνε την ανοικτή συνεργασία και επικοινωνία και περιλάμβανε μια στενή ανασκόπηση 15 υποψηφίων. Μετά από μια έντονη αξιολόγηση, το σχέδιο Rijndael, που δημιουργήθηκε από δύο Βέλγους κρυπτογράφους, ήταν η τελική επιλογή.

Το AES αντικατέστησε το DES με νέες και ενημερωμένες λειτουργίες:

- Εφαρμογή κρυπτογράφησης με μπλοκ
- Ομαδική κρυπτογράφηση μεγέθους 128-bit με κλειδιά 128, 192 και 256-bit
- Συμμετρικός αλγόριθμος που απαιτεί μόνο ένα κλειδί κρυπτογράφησης και αποκρυπτογράφησης
- Ασφάλεια δεδομένων για 20-30 χρόνια
- Παγκόσμια πρόσβαση
- Δεν περιλαμβάνει δικαιώματα
- Εύκολη συνολική εφαρμογή[71]

4.5.2 Έλεγχος Πρόσβασης

Μία από τις πιο βασικές παραμέτρους κατά τη σχεδίαση του συστήματος ιατρικής επιχειρησιακής νοημοσύνης είναι ο έλεγχος πρόσβασης στο σύστημα. Ο έλεγχος πρόσβασης εξασφαλίζει οποιαδήποτε υπηρεσία να είναι προσβάσιμη μόνο στους νόμιμους χρήστες με τα κατάλληλα προνόμια. συστήματα ηλεκτρονικής υγείας φυσικά απαιτούν λεπτόκοκκο έλεγχο των προσβάσεων. Για παράδειγμα, η πρόσβαση στην υπηρεσία που παρακολουθεί τις επιδόσεις του ασθενούς σε πραγματικό χρόνο θα πρέπει να παρέχεται μόνο σε προηγουμένως εγγεγραμμένους χρήστες που τους έχει επιτραπεί η πρόσβαση τη συγκεκριμένη χρηστή. [72][73]

Ο έλεγχος πρόσβασης με βάση ρόλο είναι ένα μηχανισμός που υιοθετήθηκε από πολλά λογισμικά υπηρεσιών στον τομέα της υγείας. Ωστόσο, εκτός των πλεονεκτημάτων που παρουσιάζει, έχει και ορισμένες αδυναμίες, όπως ότι μπορεί να επιβάλλει χρονικούς περιορισμούς, όπως η διάρκεια μιας συνεδρίας, για κάθε ρόλο αλλά όχι ανά χρήστη. Για την επιβολή περιορισμών συγκεκριμένου χρήστη απαιτείται δημιουργία ενός ρόλου για κάθε ένα χρήστη, η οποία μειώνει την αξία του ελέγχου πρόσβασης κατά τη διαχείριση ασφαλείας του συστήματος. Ο μηχανισμός

αυτός και οι τροποποιήσεις που εισάγουμε για την αποτελεσματικότερη απόδοση του αναλύονται στις παρακάτω παραγράφους[74][75].

4.5.2.1 Έλεγχος πρόσβασης με βάση το ρόλο

Ο έλεγχος πρόσβασης με βάση το ρόλο (Role Based Access Control ή εν συντομία RBAC) είναι ένας μηχανισμός ελέγχου πρόσβασης που απομπλέκει τους χρήστες του συστήματος από τα δικαιώματα τους μέσω της τοποθετήσεως ρόλων ως ενδιάμεσο στάδιο. Οι χρήστες έχουν εκχωρηθεί σε ρόλους και οι ρόλοι έχουν εξουσιοδοτηθεί για πρόσβαση σε αντικείμενα και πληροφορίες με διακριτά δικαιώματα. Αυτή η αποσύνδεση προσδίδει μεγαλύτερο βαθμό κλιμάκωσης στα συστήματα στα οποία πρέπει να ρυθμίζεται η πρόσβαση. Ένας ρόλος μπορεί να αντικατοπτρίζει τις ευθύνες μιας θέσης ή περιγραφής θέσης εργασίας στο πλαίσιο ενός οργανισμού (π.χ. Ιατρός ή νοσοκόμος). Όταν ένας χρήστης αναλαμβάνει την ευθύνη να εκτελέσει μια συγκεκριμένη εργασία μέσα στο σύστημα, ο διαχειριστής ασφαλείας τον τοποθετεί στον κατάλληλο ρόλο. Μπορούν να ασκήσουν τις εργασίες που προκύπτουν με βάση τα δικαιώματα που σχετίζονται με το ρόλο, επειδή αναγνωρίζονται ότι κατέχουν το ρόλο.

Ο έλεγχος πρόσβασης με βάση το ρόλο τυγχάνει σημαντικής προσοχής και αποδοχής στο πλαίσιο της υγειονομικής περίθαλψης, ιδιαίτερα στο νοσοκομειακό περιβάλλον. Ωστόσο, οι πρακτικές συνέπειες της εφαρμογής πολιτικών πρόσβασης που βασίζονται στη συγκατάθεση των ασθενών δεν αντιμετωπίζονται άμεσα. Οι πολιτικές πρόσβασης καθορίζονται σε επίπεδο οργανισμού ή σε επίπεδο υπηρεσιών και η δυνατότητα υποστήριξης μεμονωμένων εξαιρέσεων από τις προεπιλεγμένες πολιτικές δεν είναι υποστηριζόμενο χαρακτηριστικό. Τη λεπτομέρεια αυτή, που είναι πολύ σημαντική για τη δόμηση ενός αξιόπιστου συστήματος MBI, το οποίο έχουμε ορίσει εξ αρχής ως «ασθενοκεντρικό» την εξετάζουμε αναλυτικά παρακάτω.

4.5.2.2 Ιεραρχία των ρόλων

Στο υλοποιημένο σύστημα ιατρικής επιχειρησιακής νοημοσύνης τα επιμέρους δικαιώματα του κάθε χρήστη, πλην του διαχειριστή του συστήματος επιλέγονται από τον ασθενή μέσω της ιεράρχησης των ρόλων. Οι οδηγίες συγκατάθεσης του ασθενούς εκφράζονται μέσω της αποδοχής και της άρνησης των ιεραρχικά συναφών ρόλων που χρησιμοποιούν μια σειρά διαφορετικών ταξινομήσεων και λεπτομερειών. Γενικότερα, το μοντέλο επιτρέπει τη χρήση οποιουδήποτε αριθμού ιεραρχιών ρόλων. Μπορούν να ενωθούν ιεραρχίες με διαφορετικές ρίζες, επιτρέποντας πολυδιάστατες δομές που υποστηρίζουν σύνθετη (πολλαπλή) κληρονομιά. Το πρωτότυπο παρέχει μια βολική μέθοδο έκφρασης για τον προσδιορισμό οντοτήτων χρησιμοποιώντας δύο βασικές ιεραρχίες βασισμένες σε ρόλους:

- **Η ιεραρχία αρμοδιοτήτων των ενδιαφερομένων**: Η ιεραρχία αυτή χρησιμοποιείται ώστε αναγνωρίζει και να εντοπίζει το σύνολο των καταχωρισμένων συμμετεχόντων μερών. Η ιεραρχία περιλαμβάνει ειδικό

ρόλο για κάθε μεμονωμένο καταχωρημένο συμμετέχων άτομο. Οι μεμονωμένοι ρόλοι του κάθε χρήστη που ενεργεί για τον εαυτό του μέσα στο συνολικό υλοποιημένο σύστημα χρησιμοποιούνται για την εφαρμογή ρητής αποδοχής ή άρνησης των συγκεκριμένων ατόμων. Να σημειωθεί σε αυτό το σημείο ότι οποιοσδήποτε κόμβος στην ιεραρχία μπορεί να επιτραπεί ή να αρνηθεί ειδικά.

- **Η ιεραρχία της ένταξης σε ομάδα:** Αυτή η ιεραρχία επιτρέπει στον οργανισμό που διαχειρίζεται το σύστημα να αναγνωρίζει τα μεμονωμένα άτομα ως μέλη είτε κλινικών είτε διοικητικών ρόλων οργάνωσης[75].

Στο σύστημα MBI, η πολιτική πρόσβασης ενός ατόμου και οι προσωπικές πληροφορίες που σχετίζονται με αυτόν καταγράφονται και επιβάλλονται μέσω ενός ρόλου με επίκεντρο τον ασθενή, στον οποίο θα αναφερθούμε ως ρόλος ομάδας φροντίδας. Η εξουσιοδότηση (η οποία μπορεί να ενεργοποιήσει το ρόλο και να ασκήσει τα δικαιώματα που του αντιστοιχούν) για ένα ρόλο ομάδας φροντίδας καθορίζεται από το περιεχόμενο των επιτρεπόμενων και απαγορευμένων λιστών του ρόλου. Αυτές οι δύο λίστες περιέχουν ρόλους που εξάγονται από την ιεραρχία ρόλων αρμοδιοτήτων και αυτή της ένταξης σε ομάδα. Οι συγκεκριμένα απορριφθέντες ρόλοι παρακάμπτουν ίσους ή περισσότερο γενικούς ρόλους (δηλαδή ισοδύναμους ή χαμηλότερους σε μια ιεραρχία) στην επιτρεπόμενη λίστα.

Με απλά λόγια, το μοντέλο που προτείνουμε εφαρμόζει το αντίθετο του ελέγχου πρόσβασης με βάση το ρόλο (anti-RBAC). Εφαρμόζει δηλαδή γενική συναίνεση με ρητή άρνηση. Αυτό το anti-RBAC μοντέλο ενοποιείται με το πρότυπο RBAC που εφαρμόζει τη γενική άρνηση με ρητή συναίνεση μέσω ενός νέου αλγόριθμου εξουσιοδότησης. Αυτό επιτρέπει ένα ευέλικτο και εκφραστικό αναθεωρημένο μοντέλο που διατηρεί την κομψότητα του RBAC χωρίς την ανάγκη επιπλέον περιορισμών[75].

4.5.2.3 Αλγόριθμος εξουσιοδότησης

Στο συγκεκριμένο σύστημα ιατρικής επιχειρησιακής νοημοσύνης οι χρήστες κάνουν πάντα αιτήματα πρόσβασης μέσω του ρόλου του χρήστη που ενεργεί για τον εαυτό του. Αυτό επιβάλλεται από το σύστημα για να διασφαλιστεί ότι η ρητή συναίνεση ή άρνηση ατόμων δεν μπορεί να παρακάμπτεται μέσω μιας επιλεκτικής ενεργοποίησης ρόλου.

Οποιοσδήποτε κόμβος σε μια ιεραρχία έχει δικαιώματα πρόσβασης που επιτρέπονται ρητά, απορρίπτονται ρητά ή διφορούμενα. Η περίπτωση για ρητή αποζημίωση ή άρνηση είναι απλή - αυτός ο κόμβος αναγνωρίζεται ως ρόλος πρόσβασης χωρίς να στηρίζεται σε άλλους κόμβους της ιεραρχίας.

Ο αλγόριθμος παρουσιάζεται στο πλαίσιο της επόμενης σελίδας:

1. Consider role start. Go to step 2.

2. Does this role have explicit denial?

– if yes, then halt algorithm with access denied

– if no, go to step 3.

3. Does this role have explicit allow?

–if yes, then if this role is start, halt algorithm with access allowed

– if yes, but this role is not start

• if no more siblings, go to step 5, otherwise

• resume at step 2 with next sibling and access allowed

– if no, go to step 4.

4. For each child ‘x’ of this role,

– set role to child ‘x’

– go to step 2.

5. Has an access allowed been received?

– if yes and role is start, halt algorithm with access allowed

– if no and role is start, halt algorithm with access denied

– otherwise set role to parent’s next sibling and resume at step 2 with any received access allowed

Ένας κόμβος με μη διασαφημένη συναίνεση η άρνηση κληροδοτεί την άδεια των παιδιών του. Εάν κάποιο από τα άμεσα παιδιά του έχει ρητή άρνηση, τότε η ασάφεια του κόμβου επιλύεται και στην άρνηση. Αν αυτό δεν συμβαίνει, τότε τα παιδιά του μη διασαφημένου κόμβου πρέπει πρώτα να επιλυθούν είτε σε συναίνεση είτε σε άρνηση, και οποιαδήποτε αναδυόμενη άρνηση περνά επίσης στον διφορούμενο γονέα. Η αμφισημία του γονέα μεταφράζεται σε συναίνεση μόνο εάν κανένα από τα παιδιά δεν έχει αρνηθεί.

Οι μη διασαφημένοι κόμβοι στην ιεραρχία δεν μπορούν να επιλυθούν αν όλα τα παιδιά τους (άμεσα και απομακρυσμένα) είναι επίσης μη διασαφημένα. Σε αυτή την περίπτωση, το μοντέλο των σιωπηρών αποφάσεων άρνησης αποφασίζει ότι τα μη διασαφημένα φύλλα μπορούν να επιλυθούν αυτόματα στην άρνηση. Αυτό είναι τυποποιημένο στον παραπάνω αλγόριθμο, ο οποίος επιλύει τα δικαιώματα πρόσβασης του ρόλου με την επωνυμία start (ο ρόλος εκκίνησης είναι ο ρόλος του χρήστη που ενεργεί για τον εαυτό του, δηλαδή ο εξατομικευμένος ρόλος του χρήστη που ζητά πρόσβαση)

Τα δεδομένα αποθηκεύονται στον διακομιστή του συστήματος, συνδυάζοντας τους ρόλους της ομάδας φροντίδας με τα στοιχεία του εκάστοτε εγγράφου και εγκρίνοντας τη μεταφορά. Η επιτρεπόμενη και απαγορευμένη λίστα των καταχωρήσεων εμφανίζεται ως επιλεγμένη σε κάθε μεμονωμένη ενότητα ενός εγγράφου. Αυτό διευκολύνει τον ασθενή και τον επαγγελματία υγείας να κατανοήσουν πώς θα ελέγχεται η πρόσβαση. Διαφορετικά τμήματα ή στοιχεία του ίδιου αρχείου, μηνύματος ή εγγράφου (τα δεδομένα) ενδέχεται να έχουν διαφορετικά επίπεδα ευαισθησίας και συνεπώς θα ισχύουν διαφορετικοί όροι συναίνεσης[76][75].

4.5.3 Κατάσταση έκτακτης ανάγκης

Σε μια κατάσταση έκτακτης ανάγκης, όπως για σε μια απειλητική για τη ζωή κατάσταση για έναν αναίσθητο ασθενή, οι πάροχοι υγειονομικής περίθαλψης μπορεί να απαιτούν προσωρινή πρόσβαση στα δεδομένα ενός ασθενούς. Οι εν λόγω συμμετέχοντες πρέπει να έχουν προσωρινή εξουσιοδότηση για να αποκρυπτογραφήσουν τις προσωπικά ιατρικά δεδομένα του ασθενούς. Ενώ ο ασθενής είναι ο μόνος στο σύστημα μας ο οποίος έχει πλήρη έλεγχο του ιατρικού του ιστορικού, όπως αναφέρθηκε προηγουμένως, ο ασθενής μπορεί επίσης να μεταβιβάσει το ρόλο σε ένα μέλος της οικογένειας ή έναν φίλο. Επομένως, ένα μέλος της οικογένειας ή ένας φίλος μπορεί να διαδραματίσει ρόλο ασθενούς προκειμένου να εξουσιοδοτήσει κάποιον τρίτο να αποκτήσει πρόσβαση στο ιατρικό ιστορικό του ασθενούς[77].

Στο σύστημα μας αυτό μπορεί να επιτευχθεί με την ενθάρρυνση ενός ασθενούς να μεταβιβάσει ένα κλειδί έκτακτης ανάγκης σε ένα μέλος της οικογένειας ή έναν φίλο όταν ο ασθενής εγγραφεί για πρώτη φορά στο σύστημα. Θα του ζητηθεί να παράσχει λεπτομέρειες επαφής έκτακτης ανάγκης για ένα μέλος της οικογένειας ή έναν φίλο

και να ορίσει ένα κλειδί έκτακτης ανάγκης σε αυτό το άτομο. Η τεχνική αυτή ονομάζεται break the glass access, και ο κάτοχος του κλειδιού μπορεί να το χρησιμοποιήσει μόνο μία φορά[78].

4.5.4 Ανωνυμία

Για την ενίσχυση της ιδιωτικότητας των ασθενών στο σύστημα ιατρικής επιχειρησιακής νοημοσύνης χρειάζεται να εξασφαλίζεται η ανωνυμία του ασθενούς μέσα στο σύστημα. Αυτό επιτυγχάνεται με μια τεχνική που ονομάζεται «ψευδωνυμοποίση».

Η ψευδωνυμοποίηση (pseudonymization) είναι μια τεχνική όπου τα δεδομένα αναγνώρισης μετατρέπονται σε ένα προσδιοριστικό και στη συνέχεια αντικαθίστανται από αυτό. Το προσδιοριστικό μπορεί να συσχετιστεί μόνο με τα δεδομένα αναγνώρισης μέσω ενός συγκεκριμένου μυστικού. Η ιδιωτικότητα αφορά τη συλλογή, αποθήκευση, χρήση και αποκάλυψη προσωπικών πληροφοριών.

Δεδομένου ότι είναι απαραίτητο να αποφευχθεί η αποθήκευση προσωπικών ιατρικών πληροφοριών με το ψευδωνυμοποιημένο σύνολο δεδομένων για τη διασφάλιση της ιδιωτικής ζωής των ασθενών, μια ψευδωνυμοποιημένη βάση δεδομένων πρέπει να περιέχει τουλάχιστον δύο πίνακες, έναν από τους οποίους όλα τα προσωπικά δεδομένα διατηρούνται διαρκώς και ένα άλλο που κρατά τα ψευδώνυμα και ψευδωνυμοποιημένα δεδομένα.

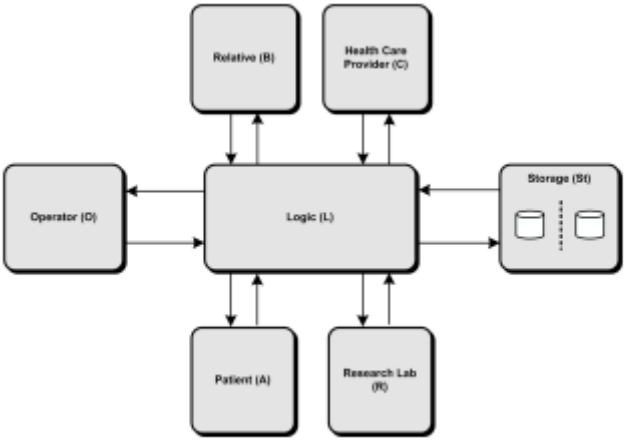
Η διαδικασία ταυτοποίησης και διαχωρισμού των προσωπικών από τα σχετικά δεδομένα ονομάζεται αποπροσωποποίηση. Μετά την αποπροσωποποίηση και την επακόλουθη ψευδωνυμοποίηση, δεν είναι δυνατή η άμεση συσχέτιση ορισμένων προσώπων με τα δεδομένα τους[79].

4.5.4.1 Η αρχιτεκτονική PIPE

Στην περίπτωση του συστήματος MBI η ψευδωνυμοποίηση επιτυγχάνεται μέσω της αρχιτεκτονικής PIPE (Pseudonymization of Information Privacy in E-health). Η αρχιτεκτονική αυτή αποτελείται από τους εξής χρήστες και υλικά:

- Ένα κεντρικό σύστημα που παρέχει πρόσβαση σε κεντρικό αποθηκευτικό χώρο, ο οποίος χωρίζεται λογικά ή και φυσικά σε δύο ξεχωριστά συστήματα αποθήκευσης (π.χ. βάσεις δεδομένων κλπ.), όπου το πρώτο σχετίζεται με τα δεδομένα αναγνώρισης και το άλλο σχετίζεται με δεδομένα, τα οποία θα πρέπει να είναι ψευδωνυμοποιημένα καθώς και το σχετικό ψευδώνυμο.
- Μια κεντρική λογική μονάδα που παρέχει μια διασύνδεση μεταξύ της κεντρικής αποθηκευτικής μονάδας και των πελατών και είναι υπεύθυνη για την αποθήκευση και φόρτωση των δεδομένων,

- Οι ασθενείς, που έχουν πλήρη πρόσβαση στα δεδομένα τους στο κεντρικό σύστημα μέσω της κεντρικής λογικής μονάδας, χρησιμοποιώντας ένα διακριτικό ασφαλείας.
- Οι ανεπίσημοι φροντιστές, οι οποίοι ενδέχεται να έχουν τα ίδια δικαιώματα με τον ασθενή από προεπιλογή, εάν δεν υπόκεινται σε τροποποίηση από το μοντέλο ελέγχου πρόσβασης.
- Οι πάροχοι υγειονομικής περίθαλψης, που μοιράζονται μία ή περισσότερες καταχωρίσεις στην ψευδωνυμοποιημένη βάση δεδομένων με τους ασθενείς
- Ο διαχειριστής που μπορεί να κρατήσει μυστικά για λογαριασμό των χρηστών[80][79].



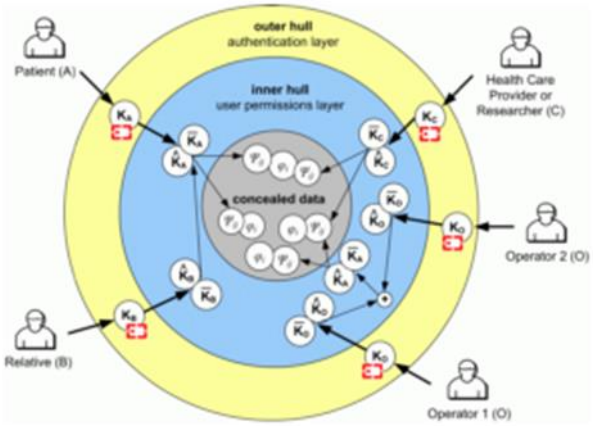
Εικόνα 7: Η αρχιτεκτονική PIPE[80]

Η αρχιτεκτονική PIPE είναι μια αρχιτεκτονική που παρέχει τις ακόλουθες συμβολές στο σύστημα σε σύγκριση με άλλες αντίστοιχες μεθοδολογίες: Συνοπτικα, η αρχιτεκτονική PIPE επιτρέπει:

- Την εξουσιοδότηση των παρόχων υγειονομικής περίθαλψης ή συγγενών των ασθενών να έχουν πρόσβαση σε καθορισμένα ιατρικά δεδομένα σε επίπεδο κρυπτογράφησης
- Την παροχή ενός ασφαλούς μηχανισμού επιστροφής, σε περίπτωση απώλειας ή φθοράς του διακριτικού ασφαλείας,
- Την αποθήκευση των δεδομένων χωρίς τη δυνατότητα κατηγοριοποίησης τους.
- Την παροχή δευτερεύουσας χρήσης χωρίς να υπάρχει σύνδεση μεταξύ των δεδομένων και του κατόχου τους[79].

Το τερματικό εν προκειμένω, είναι ουσιαστικά μια υπηρεσία που παρέχει μια διασύνδεση με εφαρμογές παλαιού τύπου, διαχειρίζεται τα αιτήματα και δημιουργεί μια ασφαλή σύνδεση με το διακομιστή. Ο διακομιστής, που ονομάζεται επίσης Λογική μονάδα, χειρίζεται τις αιτήσεις από τα τερματικά στον αποθηκευτικό. Τα δεδομένα στην αποθήκευση χωρίζονται σε δύο μέρη, τα προσωπικά δεδομένα και τα ψευδωνυμοποιημένα ιατρικά δεδομένα. Η σύνδεση μεταξύ των προσωπικών

δεδομένων και των ψευδωνυμοποιημένων ιατρικών δεδομένων προστατεύεται μέσω μιας αρχιτεκτονικής κελύφους.



Εικόνα 8: Η Αρχιτεκτονική κελύφους[81]

Η αρχιτεκτονική κελύφους περιέχει τουλάχιστον τρία επίπεδα ασφαλείας:

- το επίπεδο επαλήθευσης ταυτότητας (εξωτερικό κέλυφος)
- το επίπεδο δικαιωμάτων χρήστη (εσωτερικό κέλυφος)
- το κρυφό επίπεδο δεδομένων

Για να περάσει στο επόμενο κέλυφος, υπάρχουν ένα ή περισσότερα μυστικά, για παράδειγμα, συμμετρικά ή ασύμμετρα κλειδιά ή κρυφές σχέσεις, σε κάθε στρώμα κύτους. Η αρχιτεκτονική PIPE ορίζει τους χρήστες με διαφορετικούς ρόλους που περιλαμβάνουν τον ασθενή A, τον ανεπίσημο φροντιστή B, τον πάροχο υγειονομικής περίθαλψης C και τον διαχειριστή O[81].

Ο ασθενής είναι ο κάτοχος των δεδομένων του και έχει πλήρη έλεγχο των συνόλων δεδομένων του. Μπορεί να δει τα ιατρικά δεδομένα του, να προσθέσει και να ανακαλέσει τους παρόχους υγειονομικής περίθαλψης και μπορεί να ορίσει άλλους συμμετέχοντες, οι οποίοι έχουν τα ίδια δικαιώματα με τον εαυτό του. Οι επαγγελματίες υγείας μπορούν να εξουσιοδοτηθούν από τον ασθενή να δουν και να δημιουργήσουν υποσύνολα δεδομένων, ενώ ο διαχειριστής παρέχει ένα αντίγραφο ασφαλείας σε περίπτωση που κάποιο διακριτικό ασφαλείας πρέπει να αντικατασταθεί.

Το στρώμα επαλήθευσης περιέχει ένα ασύμμετρο ζεύγος κλειδιών, π.χ. το εξωτερικό δημόσιο κλειδί του ασθενούς K_A και το εξωτερικό ιδιωτικό κλειδί K_A^{-1}. Αυτά τα πλήκτρα αποθηκεύονται σε μια έξυπνη κάρτα και προστατεύονται με έναν κωδικό PIN. Το εξωτερικό ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση των πλήκτρων του στρώματος κύλισης άδειας.

Το επίπεδο δικαιωμάτων περιέχει ένα ασύμμετρο ζεύγος κλειδιών και ένα συμμετρικό κλειδί, δηλαδή το εσωτερικό δημόσιο κλειδί του ασθενούς $\widehat{K}_A$, το

εσωτερικό ιδιωτικό κλειδί $\widehat{K}_A^{-1}$ και το συμμετρικό κλειδί $\overline{K}_A$. Το συμμετρικό κλειδί είναι κρυπτογραφημένο με το εσωτερικό ιδιωτικό κλειδί και χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση ψευδώνυμων στο κρυφό επίπεδο δεδομένων. Εάν ένας ασθενής συνδέει έναν άλλον χρήστη, το εσωτερικό κλειδί $\widehat{K}_A^{-1}$ του πρώτου είναι κρυπτογραφημένο με το εσωτερικό δημόσιο κλειδί K_B του δεύτερου. Έτσι, ο δεύτερος χρήστης είναι σε θέση να αποκρυπτογραφήσει το συμμετρικό κλειδί $\overline{K}_A$ του ασθενούς με το εσωτερικό ιδιωτικό του κλειδί $\widehat{K}_B^{-1}$, μέχρι να αλλάξει το εσωτερικό ιδιωτικό κλειδί $\widehat{K}_A^{-1}$ του ασθενούς.

Το κρυφό επίπεδο δεδομένων περιέχει κρυφές σχέσεις, που ονομάζονται ψευδώνυμα. Κάθε σύνολο ιατρικών δεδομένων συσχετίζεται με ένα ή περισσότερα ψευδώνυμα ψ_{ij} . Καθώς ο ασθενής είναι ο νόμιμος κάτοχος των ιατρικών του δεδομένων και το άτομο με την κατάλληλη άδεια ασφαλείας από το σύστημα, κατέχει το λεγόμενο ριζικό ψευδώνυμο ψ_{i0}. Αυτά τα ψευδώνυμα υπολογίζονται με έναν αλγόριθμο, ο οποίος βασίζεται σε ένα μυστικό κλειδί. Στην περίπτωσή μας, αυτό το μυστικό κλειδί είναι το συμμετρικό κλειδί του χρήστη. Μόνο περιπτώσεις οι οποίες είναι σε θέση να αποκρυπτογραφήσουν ένα από αυτά τα ψευδώνυμα ψ_{ij} μπορούν να ανοικοδομήσουν τη σύνδεση μεταξύ του ασθενούς και των ιατρικών του δεδομένων.

Για να βρεθούν τα ψευδώνυμα ώστε να επανοικοδομηθεί η σύνδεση με τα ιατρικά δεδομένα, εισάγονται στο σύστημα κάποιες λέξεις-κλειδιά. Λέξεις-κλειδιά επιλέγονται κατά το χρόνο δημιουργίας των ιατρικών δεδομένων ή όταν ένας άλλος χρήστης είναι εξουσιοδοτημένος. Είναι κρυπτογραφημένα με το συμμετρικό κλειδί του πηγαίου χρήστη και του χρήστη, ο οποίος είναι εξουσιοδοτημένος. Αφού οι λέξεις-κλειδιά αποθηκευτούν στη βάση δεδομένων, ο χρήστης μπορεί να επιλέξει οποιαδήποτε από αυτές τις λέξεις-κλειδιά για να βρει το ψευδώνυμο[82][80].

Κεφάλαιο 5ο

Συμμόρφωση του συστήματος ιατρικής επιχειρησιακής νοημοσύνης με τους κανόνες ηθικής και δεοντολογίας

5.1 Το υπόβαθρο και οι στόχοι του HIPPA

Το πρότυπο πάνω στο όποιο έχουμε βασίσει το σχεδιασμό του συστήματος ιατρικής επιχειρησιακής νοημοσύνης και συμμορφώνεται γύρω από αυτό είναι το Health Insurance Portability and Accountability Act (HIPPA). Νομοθετήθηκε την 21η Αυγούστου 1996 ως μία δράση βελτίωσης της φορητότητας και της υπευθυνότητας σε θέματα ασφάλισης υγείας των εργαζομένων αλλά και για την καταπολέμηση της σπατάλης, της εξαπάτησης και της εκμετάλλευσης στην ιατροφαρμακευτική και υγειονομική περίθαλψη. Η δράση αυτή, επίσης, συνέβαλε στην προώθηση της δημιουργίας αποταμιευτικών λογαριασμών για ιατρικούς σκοπούς με μείωση των φόρων, στην ασφαλιστική κάλυψη εργαζομένων με προβλήματα υγείας που προϋπήρχαν της έναρξης συμβάσεως εργασία τους αλλά και στην απλούστευση της διοίκησης του χώρου της ιατρικής ασφάλισης.

Οι διαδικασίες απλούστευσης της διοίκησης του χώρου της ιατρικής ασφάλισης αποτέλεσαν το μέσο για την βιομηχανία της ιατρικής περίθαλψης ώστε να ξεκινήσει την ψηφιοποίηση των ιατρικών αρχείων των ασθενών. Το γεγονός αυτό είχε ως αποτέλεσμα τη δημιουργία του Health Information Technology for Economic and Clinical Health Act (HITECH) το 2009, η οποία με τη σειρά της παρουσίασε την πρωτοβουλία της χρήσης με σημασία (Meaningful Use), η οποία, όπως υποστηρίζεται από τους ηγέτες στον τομέα της υγειονομικής περίθαλψης και ασφάλισης, αποτελεί την πιο σημαντική νομοθεσία που θεσπίσθηκε στη βιομηχανία της περίθαλψης της Υγείας τα τελευταία 20-30 χρόνια[83][84].

5.2 Ο κανόνας απορρήτου του HIPAA

Ο κανόνας απορρήτου του HIPAA ρυθμίζει τη χρήση και δημοσιοποίηση των προστατευόμενων πληροφοριών για την υγεία του ασθενούς που βρίσκονται στα αρχεία διαφόρων παρόχων υγειονομικής περίθαλψης και άλλων ιδιωτών που προσφέρουν υπηρεσίες υγείας, οι οποίες έρχονται σε επαφή με το ιατρικό ιστορικό των ασθενών ή με πληροφορίες πληρωμών τους.

Ο Κανόνας του Απορρήτου (Privacy Rule) προτείνει πως όλοι οι παραπάνω επαγγελματίες πρέπει να ειδοποιούν τους εκάστοτε ασθενείς σχετικά με το πώς χρησιμοποιούνται οι ευαίσθητες και προστατευόμενες πληροφορίες για την υγεία τους. Ακόμη, οι ίδιοι πρέπει να κρατάνε αρχείο των δημοσιοποιήσεων των προστατευόμενων αυτών πληροφοριών αλλά και να καταγράφουν όλες τις πολιτικές απορρήτου και τις διαδικασίες σχετικά με το ιατρικό απόρρητο. Επιπρόσθετα, κρίνεται απαραίτητο να απασχολούν έναν υπεύθυνο για το απόρρητο και κάποιο

άλλο άτομο που θα καταγράφει τυχόν παράπονα αλλά και θα εκπαιδεύει όλους τους εμπλεκόμενους υπαλλήλους σχετικά με τις πολιτικές και τις διαδικασίες που αφορούν τις προστατευόμενες πληροφορίες υγείας. Συγκεκριμένα, πρέπει να λογοδοτούν πότε μια τέτοια πληροφορία μπορεί να δημοσιοποιηθεί, σε ποιόν και υπό ποιες προϋποθέσεις.

Ένας φορέας μπορεί να δημοσιοποιήσει τέτοιες ευαίσθητες πληροφορίες για να διευκολύνει δραστηριότητες που σχετίζονται με θεραπεία, πληρωμές ή ιατρική περίθαλψη χωρίς της γραπτή συναίνεση του ασθενούς. Για οποιαδήποτε άλλο λόγο δημοσιοποίησης και χρήσης των προστατευόμενων πληροφοριών υγείας είναι απαραίτητο από μεριάς του παρόχου υγειονομικής περίθαλψης να έχει την γραπτή εξουσιοδότηση του ασθενούς για τη χρήση του ιατρικού του ιστορικού. Τέλος, στην περίπτωση που χρειαστεί κάποιος πάροχος υγειονομικής περίθαλψης να δημοσιοποιήσει ιατρικές πληροφορίες του ασθενούς, πρέπει να προσπαθήσει για την ελάχιστη απαραίτητη δημοσιοποίηση όγκου των ιατρικών του πληροφοριών.

Οι πάροχοι υγειονομικής περίθαλψης μπορούν να δημοσιοποιήσουν προστατευόμενες πληροφορίες με εντολή του νόμου (συμπεριλαμβανομένων δικαστικών εντολών και κλητεύσεων) με την αρμόζουσα πάντα προστασία των προσωπικών δεδομένων του ασθενούς. Ο κανόνας περί προστασίας του απορρήτου απαιτεί από τους φορείς που έχουν υπό την κατοχή τους το ιατρικό ιστορικό ενός ασθενούς να παρέχουν αντίγραφο των δεδομένων περίθαλψης του ασθενούς εντός τριάντα (30) ημερών από την παραλαβή γραπτής αίτησης. Ακόμη, πρέπει να αποκαλύπτουν το τέτοιες πληροφορίες, όπως απαιτείται από το νόμο, σε περιπτώσεις υποψίας για κακοποίηση παιδιών, προκειμένου να επιτρέψουν στις κρατικές υπηρεσίες πρόνοιας παιδιών να εντοπίσουν έναν ύποπτο, φυγόδικο, μάρτυρα ή αγνοούμενο άτομο.

Ο κανόνας προστασίας του ιατρικού απορρήτου παρέχει στα άτομα το δικαίωμα να ζητούν από τον εκάστοτε πάροχο υγειονομικής περίθαλψης να διορθώνει τυχόν ανακρίβειες σχετικά με το ιατρικό ιστορικό τους. Απαιτεί επίσης από τους παραπάνω να λαμβάνουν μέτρα ώστε να εξασφαλιστεί η εμπιστευτικότητα των επικοινωνιών με τους ασθενείς. Εν συνεχεία, ένα άτομο που πιστεύει ότι δεν τηρείται ο κανόνας προστασίας του ιατρικού απορρήτου μπορεί να υποβάλει καταγγελία στο υπουργείο Υγείας, αλλά και στις αρμόδιες αρχές για την προστασία των προσωπικών δεδομένων και των δικαιωμάτων του πολίτη.

Στο σημείο αυτό, θα πρέπει να σημειωθεί πως ο κανόνας προστασίας του ιατρικού απορρήτου προστατεύει τις ευαίσθητες πληροφορίες του ασθενούς σε οποιαδήποτε μορφή. Περιλαμβάνει δηλαδή αρχεία υπολογιστή και έγγραφα, ακτινογραφίες, ιατρικούς λογαριασμούς, υπαγορευμένες σημειώσεις, συνομιλίες και πληροφορίες που καταγράφονται κατά την είσοδο του ασθενούς προς νοσηλεία και όχι μόνο κτα τη διάρκεια αυτής[85].

5.2.1 Χρήση και δημοσιοποίηση προστατευόμενων πληροφοριών υγείας

Ο κανόνας προστασίας του ιατρικού απορρήτου περιορίζει τον τρόπο με τον οποίο προστατευόμενες πληροφορίες μπορεί να χρησιμοποιηθούν και να αποκαλυφθούν με σκοπό να προφυλάξει τις πληροφορίες περί υγειονομικής περίθαλψης και πληρωμής των ασθενών, προσπαθώντας όμως παράλληλα να αποφύγει τη δημιουργία φραγμών που θα μπορούσαν να επηρεάσουν την παροχή υπηρεσιών υγειονομικής περίθαλψης.

Πολλοί ασθενείς κρίνουν τη χρήση και την αποκάλυψη των ιατρικών τους πληροφοριών ως αναγκαία για την παροχή θεραπείας και, σε κάποιο βαθμό, ως μέσο εξασφάλισης από πλευράς των επιχειρήσεων υγείας ότι μπορούν να λειτουργούν αποτελεσματικά. Έτσι, για να αποφευχθεί η παρεμπόδιση της πρόσβασης ενός ατόμου σε ποιοτική υγειονομική περίθαλψη ή της αποτελεσματικής πληρωμής προς τις υπηρεσίες υγειονομικής περίθαλψης, ο κανόνας προστασίας του ιατρικού απορρήτου του HIPAA επιτρέπει σε έναν πάροχο υγειονομικής περίθαλψης να χρησιμοποιεί και να αποκαλύπτει προστατευμένες πληροφορίες ιατρικού ιστορικού, υπό συγκεκριμένες προϋποθέσεις όπως για δραστηριότητες θεραπείας, πληρωμών και υγειονομικής περίθαλψης[86][87].

5.2.2 Οι απαραίτητες ελάχιστες πληροφορίες

Ένας πάροχος υγειονομικής περίθαλψης πρέπει να είναι σε θέση να αναπτύξει πολιτικές και διαδικασίες που περιορίζουν τις αποκαλύψεις και τα αιτήματα για αποκάλυψη των ιατρικών δεδομένων του ασθενούς στα ελάχιστα δεδομένα που απαιτούνται για την επίτευξη του στόχου. Απαιτείται επίσης να αναπτύξει πολιτικές και διαδικασίες πρόσβασης οι οποίες περιορίζουν τα μέλη του εργατικού δυναμικού της που μπορούν να έχουν πρόσβαση σε πληροφορίες ιατρικού απορρήτου για θεραπευτικές αγωγές, πληρωμές και υγειονομική περίθαλψη[88].

5.3 Ο κανόνας ασφαλείας του HIPPA

Ενώ ο κανόνας περί προστασίας ιατρικών προσωπικών δεδομένων του HIPAA ασχολείται με την ακεραιότητα των προστατευόμενων ιατρικών πληροφοριών εν γένει, ο κανόνας ασφαλείας του HIPAA ασχολείται με την προστασία των πληροφοριών αυτών στην ηλεκτρονική τους μορφή . Πιο συγκεκριμένα, τα ιατρικά αρχεία αξίζουν περισσότερο για τους χάκερς από τις πιστωτικές κάρτες καθώς με κλεμμένα ιατρικά αρχεία και προσωπικά αναγνωριστικά στοιχεία, οι χάκερς μπορούν να δημιουργήσουν ψευδή ταυτότητα για να λάβουν δωρεάν ιατρική περίθαλψη ή να αποκτήσουν φάρμακα που μπορούν να μεταπωληθούν στη μαύρη αγορά. Έτσι, σε συνδυασμό με έναν ψεύτικο αριθμό παρόχου, οι ασφαλιστικές εταιρείες μπορούν να τιμολογούνται για θεραπεία που δεν έχει πραγματοποιηθεί ποτέ ή για ιατρικό εξοπλισμό που δεν έχει παραδοθεί ποτέ. Επιπλέον, η κλοπή ιατρικής ταυτότητας συχνά δεν εντοπίζεται αμέσως από έναν ασθενή ή τον πάροχο υγειονομικής περίθαλψης, γεγονός που καθιστά τα ιατρικά δεδομένα πολύ πιο πολύτιμα από τις

πιστωτικές κάρτες, οι οποίες τείνουν να ακυρώνονται γρήγορα από τις τράπεζες μόλις διαπιστωθεί απάτη.

Όσον αφορά ειδικότερα τις ηλεκτρονικά αποθηκευμένες ιατρικές πληροφορίες, ο κανόνας ασφαλείας καθόρισε τρεις παραμέτρους ασφαλείας (διοικητικές, φυσικές και τεχνικές) για να περιγράψουν τη συμμόρφωση με τον Κανόνα της HIPAA. Οι παράμετροι έχουν τους ακόλουθους στόχους:

- Διοικητική παράμετρος: Έχει ως στόχο να δημιουργήσει πολιτικές και διαδικασίες που έχουν σχεδιαστεί ώστε να θέτουν με σαφήνεια τον τρόπο με τον οποίο ο πάροχος υγειονομικής περίθαλψης θα εφαρμόζει τον HIPPA.
- Φυσική παράμετρος: Έχει ως στόχο να ελέγξει τη φυσική πρόσβαση σε περιοχές αποθήκευσης δεδομένων και πώς αυτά θα προστατεύονται από τυχόν ακατάλληλη πρόσβαση.
- Τεχνική παράμετρος : Έχει ως στόχο την προστασία των ηλεκτρονικών επικοινωνιών που περιέχουν ευαίσθητα ιατρικά δεδομένα όταν αυτές πραγματοποιούνται μέσω ανοικτών δικτύων[89].

5.4 Τεχνική διασφάλιση

Όπως αναφέρθηκε και παραπάνω το σύστημα επιχειρησιακής νοημοσύνης σχεδιάστηκε και συμμορφώνεται με βάση το πρότυπο HIPPA. Αυτό σημαίνει πως χρειάζεται να πληροί συγκεκριμένες δικλείδες ασφαλείας, τα οποία το κάνουν τελικά ασφαλές στη χρήση του συνολικά. Η δομή της τεχνικής διασφάλισης και ο τρόπος που συμμορφώνεται με το πρότυπο παρουσιάζονται παρακάτω.

Έλεγχοι πρόσβασης: Αυτό σημαίνει ότι στο σύστημα επιχειρησιακής νοημοσύνης μπορεί να μπορούν να έχουν πρόσβαση μόνο εξουσιοδοτημένοι χρήστες στους οποίους έχουν χορηγηθεί δικαιώματα πρόσβασης. Επίσης, σχετικά με τον έλεγχο πρόσβασης των χρηστών εφαρμόζονται μηχανισμοί που εντοπίζουν και παρακολουθούν τη δραστηριότητα των χρηστών, καταγράφουν αυτόματα τον χρήστη μετά από μια περίοδο αδράνειας και επιτρέπουν την πρόσβαση στα δεδομένα του ασθενούς στο MBI σε περίπτωση έκτακτης ανάγκης[90].

Διενέργεια ελέγχων: Πρόκειται για γενικούς ελέγχους που τίθενται σε εφαρμογή για την παρακολούθηση, καταγραφή και εξέταση όλων των δραστηριοτήτων που αφορούν το σύστημα. Κατ' επέκταση συνιστάται να διαμορφώνονται έτσι ώστε να συμπληρώνουν τους υφιστάμενους μηχανισμούς για τις καταγραφές ιατρικών δεδομένων ηλεκτρονικά (Electronic Health Records) και μπορούν να χρησιμοποιηθούν για τη διεξαγωγή των αξιολογήσεων κινδύνου, για να προσαρμόσουν τους ελέγχους πρόσβασης των χρηστών αλλά και τις πολιτικές που αφορούν το προσωπικό ανάλογα πάντοτε με τις ανάγκες της χρονικής συγκυρίας[91].

Ακεραιότητα: Η διατήρηση της ακεραιότητας του συστήματος MBI σημαίνει ότι δεν καταστρέφεται ή μεταβάλλεται, συνολικά ή κατά περίπτωση, με τρόπο που δεν

συμμορφώνεται με το πρότυπο HIPAA. Έτσι, πρέπει η εμπλεκόμενη αρχή παροχής ιατρικής περίθαλψης να διαβεβαιώνει ότι η πρόσβαση σε δεδομένα γίνεται σωστά και μόνο από εξουσιοδοτημένους χρήστες[92].

Έλεγχος ταυτότητας προσώπου ή φορέα: Αυτός ο έλεγχος χρησιμεύει στο να εξασφαλιστεί η ταυτοπροσωπία του ατόμου που επιθυμεί πρόσβαση στο σύστημα. Αυτό επιτυγχάνεται με τη διανομή κωδικών πρόσβασης ή κωδικών PIN από έναν διορισμένο διαχειριστή, ο οποίος έχει τη δυνατότητα να κλειδώνει με PIN μια συσκευή, εάν η αξιολόγηση κινδύνου δείξει ότι υπάρχει απειλή παραβίασης του συστήματος ή απώλεια ή κλοπή μιας συσκευής.

Ασφάλεια μεταφοράς: Η ασφάλεια του συστήματος κατά τη διάρκεια της μεταφοράς πληροφοριών θα πρέπει να καθορίζεται με τη χρήση κρυπτογράφησης δεδομένων. Το σύστημα θα πρέπει να καθίσταται ακατάλληλο, ανυπόγραφο ή άχρηστο, έτσι ώστε οι πληροφορίες περί υγειονομικής περίθαλψης ή πληρωμής ασθενών να μην είναι χρήσιμες σε μη εξουσιοδοτημένο τρίτο άτομο ή φορέα. Η αποτελεσματική κρυπτογράφηση βοηθά επίσης τους εμπλεκόμενους φορείς να αποφύγουν σημαντικό πρόστιμο σε περίπτωση παραβίασης των ιατρικών δεδομένων του ασθενούς[91].

5.4.1 Φυσικοί Έλεγχοι

Κατά την εγκατάσταση του συστήματος ιατρικής επιχειρησιακής νοημοσύνης, τόσο στο χώρο που βρίσκεται η κεντρική εγκατάσταση (π.χ. Server room), όσο και στους χώρους που προβλέπεται να γίνεται η χρήση του από τον ασθενή, πραγματοποιείται μια σειρά από φυσικούς ελέγχους, που εξασφαλίζουν τη σωστή και ασφαλή λειτουργία του. Οι φυσικοί έλεγχοι που πραγματοποιούνται είναι οι εξής:

Έλεγχοι πρόσβασης εγκατάστασης: Οι έλεγχοι πρόσβασης των εγκαταστάσεων περιγράφουν τις πολιτικές και τις διαδικασίες που πρέπει να εφαρμόζουν οι πάροχοι υγειονομικής περίθαλψης για να πιστοποιήσουν την ταυτότητα και να επιτρέψουν την πρόσβαση σε χώρους όπου στεγάζονται τα δεδομένα του συστήματος MBI. Σήμερα αυτό σημαίνει τη θέσπιση κατάλληλων διαδικασιών για να διασφαλιστεί ότι μόνο το εξουσιοδοτημένο προσωπικό θα μπορεί να έχει πρόσβαση σε κέντρα δεδομένων, σε διακομιστές, σε αποθήκες και σε οποιεσδήποτε άλλους χώρους όπου αποθηκεύονται δεδομένα του, ή υπάρχουν μέρη του συστήματος. Αυτό περιλαμβάνει ακόμη αποθήκες όπου διατηρείται παλαιότερος εξοπλισμός του συστήματος πληροφορικής που δεν χρησιμοποιείται πλέον. Επίσης, θα πρέπει να ελέγχεται η πρόσβαση σε ψηφιακές συσκευές οι οποίες περιέχουν αποθηκευμένα δεδομένα, συμπεριλαμβανομένων των ψηφιακών φωτοαντιγραφικών συσκευών, των σαρωτών και των εκτυπωτών[93].

Χρήση του χώρου εργασίας: Τα πρότυπα που εφαρμόζονται σχετικά με τους χώρους εργασίας στους οποίους φιλοξενούνται οι πάροχοι υγειονομικής περίθαλψης ορίζουν τί μπορεί να χρησιμοποιηθεί σε κάθε χώρο εργασίας, πώς εκτελείται η

εργασία στο χώρο εργασίας καθώς και το περιβάλλον που περιβάλλει τους χώρους εργασίας όταν χρησιμοποιούνται για πρόσβαση στα δεδομένα του χώρου εργασίας.

Ασφάλεια χώρου εργασίας: Η ασφάλεια του χώρου εργασίας είναι στενά συνδεδεμένη με τα πρότυπα χρήσης του χώρου εργασίας που αναφέρθηκαν παραπάνω, αλλά υπάρχει σημαντική διάκριση μεταξύ των δύο καθώς το πρώτο χρησιμοποιεί τις πολιτικές και τις διαδικασίες για τον τρόπο χρήσης των χώρων εργασίας, ενώ το πρότυπο ασφαλείας του χώρου εργασίας εξετάζει τον τρόπο με τον οποίο οι χώροι εργασίας πρέπει να προστατεύονται φυσικά από μη εξουσιοδοτημένους χρήστες[93].

Έλεγχοι των συσκευών και των ηλεκτρονικών μέσων: Το τέταρτο και τελικό πρότυπο στο σχετικά με τους φυσικούς ελέγχους είναι ο έλεγχος συσκευών και μέσων. Το πρότυπο αυτό καλεί τους παρόχους υγειονομικής περίθαλψης να εφαρμόσουν τις πολιτικές και τις διαδικασίες που είναι απαραίτητες για την παραλαβή και την απομάκρυνση του υλικού από και προς σε κάποια υποδομή καθώς και των ηλεκτρονικών μέσων που περιέχουν ηλεκτρονικές προστατευμένες πληροφορίες για την υγεία. Αυτό φυσικά δεν περιορίζεται μόνο στις συσκευές που υπάρχουν στο χώρο του παρόχου, αλλά αφορά ασφαλώς και τις συσκευές που χρησιμοποιεί ο ασθενής για την πρόσβασή του στο σύστημα[83].

5.5 Διοικητικές παράμετροι ασφαλείας

Για την αποτελεσματική λειτουργία του συστήματος ιατρικής επιχειρησιακής νοημοσύνης, πέραν των μηχανισμών και των τεχνικών που χρησιμοποιήθηκαν και περιγράφονται σε προηγούμενο κεφάλαιο, αλλά και των φυσικών ελέγχων που εφαρμόζονται, εφαρμόζονται στο σύστημα, όπως ορίζει το πρότυπο HIPPA, μια σειρά από διοικητικές παραμέτρους ασφαλείας που εξασφαλίζουν την εύρυθμη λειτουργία του.

5.5.1 Διαδικασία Διαχείρισης Ασφάλειας

Η διαδικασία διαχείρισης ασφάλειας καλύπτει την εφαρμογή διαδικασιών αναφορικά με την πρόληψη, ανίχνευση, περιορισμό και διόρθωση παραβιάσεων ασφαλείας.

Αυτά κατηγοριοποιούνται σε 4 παραμέτρους εφαρμογής:

- Ανάλυση Κινδύνου (Απαιτείται)
- Διαχείριση κινδύνων (Απαιτείται)
- Πολιτική κυρώσεων (Απαιτείται)
- Ανασκόπηση δραστηριότητας του συστήματος πληροφοριών (Απαιτείται)

Το σύστημα MBI λοιπόν προβλέπει την αναγκαιότητα διορισμού υπάλληλου ασφαλείας (μέλος της ομάδας του διαχειριστή του συστήματος) ο οποίος

αναλαμβάνει την ευθύνη για την ανάπτυξη και εφαρμογή των διαδικασιών του προτύπου HIPAA σχετικά με την ασφάλεια των δεδομένων.

5.5.2 Ασφάλεια εργατικού δυναμικού

Μολονότι η πρόσβαση στο σύστημα MBI πρέπει να περιορίζεται και να ελέγχεται προσεκτικά, οι επαγγελματίες του τομέα υγείας χρειάζονται πρόσβαση σε αυτό για να διεκπεραιώσουν διάφορες εργασίες, όπως τη διαχείριση και το σχεδιασμό των παιχνιδιών και την αξιολόγηση του ασθενούς, ως μέρος της παροχής υγειονομικής περίθαλψης σε αυτόν. Αυτό σημαίνει ότι έχουν αναπτυχθεί πολιτικές και διαδικασίες για να εξασφαλιστεί ότι όλα τα μέλη του εργατικού δυναμικού θα έχουν κατάλληλη πρόσβαση στο σύστημα MBI, όπως προβλέπεται στο πρότυπο διαχείρισης της πρόσβασης στις πληροφορίες. Από την άλλη, θα πρέπει να αποτρέπεται η έκθεση στα δεδομένα του συστήματος των συμμετεχόντων που δεν κατέχουν την κατάλληλη εξουσιοδότηση.

Η ασφάλεια του εργατικού δυναμικού περιλαμβάνει τρεις παραμέτρους εφαρμογής:

- Εξουσιοδότηση ή / και εποπτεία
- Διαδικασία εκκαθάρισης εργατικού δυναμικού
- Διαδικασίες τερματισμού αρχείων

5.5.3 Διαχείριση πρόσβασης στις πληροφορίες

Το πρότυπο αυτό καλύπτει τη διαχείριση της πρόσβασης στο MBI από τα μέλη του εργατικού δυναμικού που πρέπει να βλέπουν, τροποποιούν ή επικαιροποιούν τα δεδομένα στο πλαίσιο των καθημερινών τους καθηκόντων. Ο έλεγχος της πρόσβασης αποτελεί ουσιαστικό στοιχείο της ασφάλειας των δεδομένων που περιορίζει τις πιθανότητες ακούσιας ή και εσκεμμένης αποκάλυψης ευαίσθητών ιατρικά πληροφοριών σε μη εξουσιοδοτημένα άτομα, περιορίζοντας παράλληλα τη δυνατότητα διαγραφής ή τροποποίησης τους.

Η διαχείριση της πρόσβασης στις πληροφορίες περιλαμβάνει τρεις παραμέτρους εφαρμογής:

- Απομόνωση λειτουργιών
- Αδειοδότηση πρόσβασης
- Δημιουργία και τροποποίηση πρόσβασης

5.5.4 Ενημέρωση ασφάλειας και κατάρτιση

Ένα από τα σημαντικότερα στοιχεία των διοικητικών παραμέτρων ασφαλείας είναι η παροχή κατάρτισης σχετικά με τους κανόνες ασφάλειας και ιδιωτικής ζωής που αναφέρονται στην HIPAA, όχι μόνο για το προσωπικό στο οποίο έχει χορηγηθεί πρόσβαση στο ePHI ή με άλλο τρόπο μπορεί να έρθει σε επαφή μαζί του, αλλά για όλα τα μέλη του εργατικού δυναμικού. Ακόμη και οι πιο ισχυρές πολιτικές ασφαλείας

μπορούν εύκολα να διακυβευτούν εξαιτίας της κακής ή ανύπαρκτης κατάρτισης του προσωπικού.

Η τήρηση της ασφάλειας και η κατάρτιση του εργατικού δυναμικού περιλαμβάνουν τρεις συγκεκριμένες εφαρμογές:

- Υπενθυμίσεις ασφαλείας
- Προστασία από κακόβουλο λογισμικό
- Παρακολούθηση σύνδεσης

5.6 Διαδικασίες αναφοράς περιστατικών ασφαλείας και σχεδιασμός έκτακτης ανάγκης

Ακόμη και οι πιο συνειδητοποιημένοι πάροχοι υγειονομικής περίθαλψης που έχουν εφαρμόσει συστήματα ασφαλείας πολλαπλών επιπέδων και είναι πλήρως συμβατοί με το HIPAA, θα βιώσουν, σε κάποιο χρονικό σημείο, ένα περιστατικό ασφάλειας. Έτσι, ενώ είναι δυνατόν να μειωθεί και να διαχειριστεί ο κίνδυνος, δεν είναι δυνατόν να το εξαλειφθεί εξ ολοκλήρου. Συνεπώς, οι εμπλεκόμενοι πάροχοι υγειονομικής περίθαλψης πρέπει να εφαρμόζουν διαδικασίες που επιτρέπουν αφενός την ταχεία αναφορά αυτών των περιστατικών και αφετέρου στο κατάλληλο προσωπικό.

Υπάρχει μόνο μία παράμετρος εφαρμογής:

- Απάντηση και αναφορά του περιστατικού (απαιτείται)

Η πρόσβαση στα δεδομένα του συστήματος πρέπει να διατηρείται ανά πάσα στιγμή, και ειδικά σε καταστάσεις έκτακτης ανάγκης. Συνεπώς, πρέπει να αναπτυχθούν διαδικασίες ώστε να διασφαλιστεί η πρόσβαση αυτή καθώς και ότι οι πάροχοι υγειονομικής περίθαλψης έχουν θεσπίσει (και εφαρμόζουν κατά περίπτωση) πολιτικές και διαδικασίες για την αντιμετώπιση περιστατικών έκτακτης ανάγκης ή άλλων περιστατικών(π.χ. πυρκαγιά, βανδαλισμό, βλάβη συστήματος και φυσική καταστροφή) που βλάπτουν τα επιμέρους συστήματα που περιέχουν ευαίσθητες ιατρικά πληροφορίες.

Ο σχεδιασμός έκτακτης ανάγκης περιλαμβάνει πέντε παραμέτρους εφαρμογής [94]:

- Σχέδιο δημιουργίας αντιγράφων ασφαλείας δεδομένων
- Σχέδιο αποκατάστασης καταστροφών
- Σχέδιο λειτουργίας έκτακτης ανάγκης
- Διαδικασίες ελέγχου και αναθεώρησης
- Εφαρμογές και Ανάλυση Κρίσιμων Δεδομένων

Κεφάλαιο 6ο

Επίλογος-Συμπεράσματα

Είναι γεγονός ότι η σωστή και αποτελεσματική περίθαλψη των ασθενών με Πάρκινσον είναι υψίστης σημασίας για την βελτίωση της προσωπικής τους ζωής και εν γένει της καθημερινότητας τους. Αν και στη διεθνή βιβλιογραφία υπάρχουν αρκετές μελέτες σχετικά με την ασφάλεια συστημάτων ηλεκτρονικής υγείας, μέχρι στιγμής δεν έχει υπάρξει κάποιο ολοκληρωμένο πρόγραμμα παρακολούθησης και αποκατάστασης των ατόμων που πάσχουν από Πάρκινσον, το οποίο να βασίζεται σε καινοτόμες τεχνολογίες επικοινωνιών και πληροφορικής.

Το σύστημα ιατρικής επιχειρησιακής νοημοσύνης (MBI), που παρουσιάστηκε σε αυτή την εργασία, συνιστά μια εναλλακτική πρόταση και δίνει μια κατεύθυνση, μέσω συγκεκριμένων κανόνων και προδιαγραφών, ως προς τη διαδικασία που απαιτείται για την ασφάλεια ενός τέτοιου συστήματος. Ειδικότερα, με τη βοήθεια των τεχνικών και των μεθόδων που χρησιμοποιήθηκαν για την ασφάλεια των δεδομένων και τον έλεγχο πρόσβασης σε αυτά, αποκτάται μια σαφής εικόνα της κατάστασης του ασθενούς σε πραγματικό χρόνο, ενώ παράλληλα δίνεται η δυνατότητα στους επιβλέποντες ιατρούς και θεραπευτές για συνεχή και έγκαιρη ενημέρωση σχετικά με την εξέλιξη της νόσου. Έτσι μπορούν να σχεδιάσουν ένα πιο εξατομικευμένο πλάνο αποκατάστασης.

Μελλοντικές επεκτάσεις και βελτιώσεις του συστήματος μπορούν να γίνουν στα περισσότερα μέρη του συστήματος, ανάλογα με την εξέλιξη της τεχνολογίας. Επιπρόσθετα, μεγαλύτερη έμφαση θα πρέπει να δοθεί στην ανάπτυξη πιο εξειδικευμένων μεθόδων ταυτοποίησης του χρήστη με βιομετρικά χαρακτηριστικά, ώστε να παρέχουν όσο το δυνατόν ποιοτικότερες προτάσεις για το σχεδιασμό της ασφάλειας του συστήματος.

Με βάση όλα τα παραπάνω, η παρούσα εργασία θα μπορούσε να αποτελέσει, τη βάση για την ανάπτυξη παρόμοιων συστημάτων που θα βοηθούν άτομα με παραπλήσιες ανάγκες (πχ: πρόβλεψη πτώσης ηλικιωμένων), αλλά και ένα χρηστικό εργαλείο για ιατρούς και θεραπευτές σχετικά με τη βοήθεια που μπορεί να τους δώσει η τεχνολογία για την εξ αποστάσεως και καλύτερη αποκατάσταση των ασθενών.

Τέλος, οι πληροφορίες που χρησιμοποιήθηκαν στην παρούσα διπλωματική προέρχονται, από απαντήσεις που έδωσαν ενδιαφερόμενοι και πιθανοί χρήστες του συστήματος (ιατροί, ασθενείς, θεραπευτές, ανεπίσημοι φροντιστές κτλ.), από επαναχρησιμοποίηση προγενέστερης γνώσης σε παρόμοια συστήματα και από αποτελέσματα και δεδομένα σχετικής διεθνούς βιβλιογραφίας.

Βιβλιογραφία

[1] C. Division, “Implementing e-Health in Developing Countries Guidance and Principles,” no. September, 2008.

[2] H. Oh, C. Rizo, M. Enkin, A. Jadad, R. F. E. Building, and E. Street, “What Is eHealth (3): A Systematic Review of Published Definitions Corresponding Author :,” vol. 7, no. 3, pp. 1–12, 2005.

[3] D. Mea and V. Della Mea, “What is e-Health (2): The death of telemedicine ?,” vol. 3, no. 2, pp. 2–3, 2001.

[4] G. Eysenbach, “What is e-health?,” *J. Med. Internet Res.*, vol. 3, no. 2, pp. 1–5, 2001.

[5] T. L. Diepgen, “in the 21st Century,” no. 0.

[6] T. Sahama and L. Simpson, “Security and Privacy in eHealth : is it possible ? A sociotechnical analysis,” no. October, 2013.

[7] E. Frontoni, M. Baldi, and P. Zingaretti, “Security issues for data sharing and service interoperability in eHealth systems : the Nu . Sa . test bed,” no. August, 2014.

[8] G. Kleiner-Fisman, P. Gryfe, and G. Naglie, “A patient-based needs assessment for living well with Parkinson disease: Implementation via nominal group technique,” *Parkinsons. Dis.*, vol. 2013, pp. 11–13, 2013.

[9] J. Jankovic, “Parkinson ’ s disease : clinical features and diagnosis,” no. 1957, pp. 368–376, 2008.

[10] EFN, “eHealth Stakeholder Group Report eSkills and Health Workforce,” no. November, 2014.

[11] P. N. Klöcker, R. Bernnat, and D. J. Veit, “Stakeholder behavior in national eHealth implementation programs,” *Heal. Policy Technol.*, vol. 4, no. 2, pp. 113–120, 2015.

[12] T. World and H. Report, “for health,” 2006.

[13] A. Barakat, R. D. Woolrych, A. Sixsmith, W. D. Kearns, and H. S. M. Kort, “eHealth Technology Competencies for Health Professionals Working in Home Care to Support Older Adults to Age in Place: Outcomes of a Two-Day Collaborative Workshop.,” *Med. 2.0*, vol. 2, no. 2, p. e10, 2013.

[14] H. Christie, “Implementation determinants of eHealth interventions for caregivers of people with dementia A systematic review.”

[15] M. E. Cooley *et al.*, “Patient and caregiver perspectives on decision support for symptom and quality of life management during cancer treatment: Implications for eHealth,” *Psychooncology.*, vol. 26, no. 8, pp. 1105–1112, Aug. 2017.

[16] “eHealth Administration Overview,” no. October, pp. 1–28, 2006.

[17] "CA Health ®."

[18] S. De Lusignan, S. Wells, P. Johnson, K. Meredith, and E. Leatham, "Compliance and effectiveness of 1 year's home telemonitoring. The report of a pilot study of patients with chronic heart failure," *Eur. J. Heart Fail.*, vol. 3, no. 6, pp. 723–730, 2001.

[19] D. Johnson and J. Wiles, "Effective affective user interface design in games," *Ergonomics*, vol. 46, no. 13–14, pp. 1332–1345, 2003.

[20] R. W. Grant *et al.*, "Design and Implementation of a Web-Based Patient Portal Linked to an Ambulatory Care Electronic Health Record: *Patient Gateway* for Diabetes Collaborative Care," *Diabetes Technol. Ther.*, vol. 8, no. 5, pp. 576–586, Oct. 2006.

[21] I. Kouris *et al.*, "KINOPTIM: The medical business intelligence module for fall prevention of the elderly," in *2015 IEEE 15th International Conference on Bioinformatics and Bioengineering (BIBE)*, 2015, pp. 1–4.

[22] T. Y. Dn and T. Yyepg, "Asking questions: A practical guide to questionnaire designSudman, S., & Bradburn, N.M. (1982). San Francisco: Jossey-Bass Publishers.," *Comput. Environ. Urban Syst.*, vol. 14, pp. 72–72, 1990.

[23] D. J. BRAMBILLA and S. M. McKINLAY, "A COMPARISON OF RESPONSES TO MAILED QUESTIONNAIRES AND TELEPHONE INTERVIEWS IN A MIXED MODE HEALTH SURVEY1," *Am. J. Epidemiol.*, vol. 126, no. 5, pp. 962–971, Nov. 1987.

[24] W. F. Boh, "Reuse of knowledge assets from repositories: A mixed methods study," *Inf. Manag.*, vol. 45, no. 6, pp. 365–375, Sep. 2008.

[25] R. Ceravolo, D. Frosini, C. Rossi, and U. Bonuccelli, "Impulse control disorders in Parkinson's disease: definition, epidemiology, risk factors, neurobiology and management," *Parkinsonism Relat. Disord.*, vol. 15, pp. S111–S115, Dec. 2009.

[26] A. R. Da Silva, "Patterns for better Use Case Specification," *Proc. Eur. 2015*, 2015.

[27] A. Cockburn, "Humans and Technology in preparation for Addison-Wesley Longman," vol. 3, 2000.

[28] G. Schneider and J. P. Winters, *Applying use cases : a practical guide*. Addison-Wesley, 1998.

[29] J. Heumann, "Tips for writing good use cases," *Tips Writ. good use cases.*, no. May, pp. 1–16, 2008.

[30] B. C. Stahl, M. Shaw, and N. Doherty, "Information Systems Security Management : A Critical Research Agenda," *Work. Inf. Secur. Priv.*, pp. 5--1–5--22, 2008.

[31] M. Veeningen, B. De Weger, and N. Zannone, "Information Systems Security," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7093. pp. 235–

249, 2011.

[32] S. Mishra and G. Dhillon, “Information Systems Security Governance Research: A Behavioral Perspective,” *1st Annu. Symp. Inf. Assur.*, pp. 27–35, 2006.

[33] S. Flowerday and R. von Solms, “Trust: An Element of Information Security,” Springer, Boston, MA, 2006, pp. 87–98.

[34] “Entrust ® White Paper The Concept of Trust in Network Security,” 2000.

[35] H. Asgari, S. Haines, and O. Rysavy, “Identification of Threats and Security Risk Assessments for Recursive Internet Architecture,” *IEEE Syst. J.*, vol. 12, no. 3, pp. 2437–2448, Sep. 2018.

[36] “Identifying Cybersecurity Threats & Evaluating IT Controls JODY CEDOLA, SENIOR IT AUDIT PROGRAM MANAGER ROBERT KALER, GROUP INTERNAL AUDIT PROGRAM MANAGER.”

[37] J. Andress, *The basics of information security : understanding the fundamentals of InfoSec in theory and practice*. .

[38] T. Sahama, L. Simpson, and B. Lane, “Security and Privacy in eHealth: Is it possible?,” *2013 IEEE 15th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2013*, no. October, pp. 249–253, 2013.

[39] D. G. O’Brien and W. A. Yasnoff, “Privacy, confidentiality, and security in information systems of state health agencies.,” *Am. J. Prev. Med.*, vol. 16, no. 4, pp. 351–8, May 1999.

[40] L. Chao, Ed., *Handbook of Research on Cloud-Based STEM Education for Improved Learning Outcomes*. IGI Global, 2016.

[41] T. H. Hotel and C. Place, “The Hilton Hotel, Charlemont Place, Dublin 2,” no. May, 2015.

[42] F. Zafar *et al.*, “A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends,” *Comput. Secur.*, vol. 65, no. 3, pp. 29–49, Mar. 2017.

[43] M. Imran, H. Hlavacs, I. U. Haq, B. Jan, F. A. Khan, and A. Ahmad, “Provenance based data integrity checking and verification in cloud environments.,” *PLoS One*, vol. 12, no. 5, p. e0177576, 2017.

[44] A. Jøsang, “A consistent definition of authorization,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10547 LNCS, no. September, pp. 134–144, 2017.

[45] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

[46] R. L. Krutz and R. D. Vines, *Cloud security : a comprehensive guide to secure cloud computing*. Wiley Pub, 2010.

[47] G. Loukas and G. ¨ Ulay¨okeulay¨ Ulay¨oke, “Protection against Denial of

Service Attacks: A Survey."

[48] S. Brands, "Privacy and Security in Electronic Health," *Security*, pp. 1–12, 2003.

[49] A. Sunyaev, T. Dehling, P. L. Taylor, and K. D. Mandl, "Availability and quality of mobile health app privacy policies," *J. Am. Med. Informatics Assoc.*, vol. 22, no. e1, pp. e28–e33, 2015.

[50] L. Ackerman, "Mobile Health and Fitness Applications and Information Privacy. Report to California Consumer Protection Foundation," *Priv. Rights Clear.*, pp. 1–26, 2013.

[51] N. Giesinger and B. Jameson, "eHealth Saskatchewan Security Policy Framework," 2011.

[52] A. Boonyarattaphan, Y. Bai, S. Chung, and R. Poovendran, "Spatial-Temporal Access Control for E-health Services," in *2010 IEEE Fifth International Conference on Networking, Architecture, and Storage*, 2010, pp. 269–276.

[53] S. Khoja, H. Durrani, P. Nayani, and A. Fahim, "Scope of policy issues in eHealth: results from a structured literature review.," *J. Med. Internet Res.*, vol. 14, no. 1, p. e34, Feb. 2012.

[54] M. Al Ameen, J. Liu, and K. Kwak, "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications," *J. Med. Syst.*, vol. 36, no. 1, pp. 93–101, Feb. 2012.

[55] F. Kargl, E. Lawrence, M. Fischer, and Y. Y. Lim, "Security, privacy and legal issues in pervasive eHealth monitoring systems," *Proc. - 7th Int. Conf. Mob. Business, ICMB 2008, Creat. Converg.*, no. February, pp. 296–304, 2008.

[56] H. Elayan, R. M. Shubair, and A. Kiourti, "Wireless sensors for medical applications: Current status and future challenges," *2017 11th Eur. Conf. Antennas Propagation, EUCAP 2017*, no. October, pp. 2478–2482, 2017.

[57] J. Hou, B. Chang, D. K. D. Cho, and M. Gerla, "Minimizing 802.11 interference on zigbee medical sensors," *Proc. Fourth Int. Conf. Body Area Networks*, p. 5, 2009.

[58] A.-M. Rahmani *et al.*, "Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems," in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 2015, pp. 826–834.

[59] A. M. Rahmani *et al.*, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 641–658, Jan. 2018.

[60] S. R. Moosavi *et al.*, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 64, no. November 2018, pp. 108–124, 2016.

[61] N. Modadugu and E. Rescorla, "Datagram Transport Layer Security."

[62] N. Koblitz, “Elliptic curve cryptosystems,” *Math. Comput.*, vol. 48, no. 177, pp. 203–203, Jan. 1987.

[63] M. Peck and K. Igoe, “Suite B Profile for Datagram Transport Layer Security / Secure Real-time Transport Protocol (DTLS-SRTP).”

[64] S. R. Moosavi *et al.*, “SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways,” *Procedia Comput. Sci.*, vol. 52, no. 1, pp. 452–459, 2015.

[65] E. B. Barker, D. Johnson, and M. E. Smid, “Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography,” Gaithersburg, MD, 2007.

[66] M. Zheng, H. Zhou, and J. Chen, “An efficient protocol for two-party explicit authenticated key agreement,” *Concurr. Comput.*, vol. 27, no. 12, pp. 2954–2963, 2015.

[67] NIST, “FIPS PUB 186-4 Digital Signature Standard (DSS) CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY,” no. July, 2013.

[68] T. Pornin, “Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA),” 2013.

[69] “Federal Information Processing Standards Publication 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES),” 2001.

[70] *ISO/IEC 18033-3:2010 - Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers*. .

[71] J. Daemen, V. Rijmen, and K. U. Leuven, “AES Proposal.”

[72] Roger Clarke, “eConsent: A critical element of trust in ebusiness.”

[73] H. Grain, “e-Consent design and implementation issues for health information managers.”

[74] D. Ferraiolo and R. Kuhn, “Role-Based Access Controls.” pp. 554–563, 13-Oct-1992.

[75] J. Reid, I. Cheong, M. Henricksen, and J. Smit, “A novel use of RBAC to protect privacy in distributed health care information systems,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2727 LNCS, pp. 403–415, 2003.

[76] A. A. Elliott and G. S. Knight, “Role Explosion: Acknowledging the Problem.”

[77] A. Sahi, D. Lai, and Y. Li, “Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan,” *Comput. Biol. Med.*, vol. 78, pp. 1–8, 2016.

[78] B. Yüksel, A. Küpçü, and Ö. Özkasap, “Research issues for privacy and security of electronic health services,” *Futur. Gener. Comput. Syst.*, vol. 68, pp. 1–13, 2017.

[79] B. Riedl, V. Grascher, S. Fenz, and T. Neubauer, "Pseudonymization for improving the privacy in e-health applications," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1–10, 2008.

[80] B. Riedl, V. Grascher, and T. Neubauer, "A secure e-health architecture based on the appliance of pseudonymization," *J. Softw.*, vol. 3, no. 2, pp. 23–32, 2008.

[81] B. I. Dmitriev, V. M. Demidov, V. E. Vansovich, and P. G. Burlaka, "Primenenie laparoskopicheskoi kholetsistektomii v lechenii zhelchnokamennoi bolezni.," *Klin. khirurhiia / Minist. okhorony zdorov'ia Ukra??ny, Nauk. tovarystvo khirurhiv Ukra??ny*, vol. 2, no. 9–10, pp. 103–104, 1997.

[82] B. Riedl, T. Neubauer, G. Goluch, O. Boehm, G. Reinauer, and A. Krumboeck, "A secure architecture for the pseudonymization of medical data," *Proc. - Second Int. Conf. Availability, Reliab. Secur. ARES 2007*, pp. 318–324, 2007.

[83] S. Requirement and I. Specifications, "Device and Media Controls TMA Privacy Office Information Paper Device and Media Controls TMA Privacy Office Information Paper," pp. 2–3.

[84] "TMA Privacy Office Information Paper," no. April 2010, 2009.

[85] H. I. Portability *et al.*, "TMA Privacy Office Information Paper TMA Privacy Office Information Paper," no. March, pp. 1–3, 2010.

[86] C. L. Office, "TMA Privacy and Civil Liberties Office Information Paper," *Best Pract. Disposing PHI*, no. September, p. 3, 2011.

[87] I. Definitions, "Best Practices : Transporting PII or PHI," 1974.

[88] A. Is and N. O. T. Required, "TMA Privacy and Civil Liberties Office Information Paper AUTHORIZATION IS NOT REQUIRED THE MINIMUM NECESSARY RULE," 2012.

[89] Defense Health Agency, "Overview of the HIPAA Security Rule HIPAA Security Information Paper," *Defending Priv.*, 2007.

[90] Microsoft, "Access Controls," vol. 306, no. d, p. 1, 2016.

[91] J. R. Silvers, "Administrative safeguards," *Risk Manag. Meet. Events*, pp. 157–183, 2008.

[92] "Integrity Standards TMA Privacy Office Information Paper," vol. 312, no. c, p. 22041.

[93] S. Requirement and I. Specifications, "Facility Access Controls TMA Privacy Office Information Paper Facility Access Controls TMA Privacy Office Information Paper," pp. 2–4.

[94] T. Health and I. Portability, "Specifications : Standards & Implementation," pp. 1–3.