Δ.Π.Μ.Σ. ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

Μεταπτυχιακή Διπλωματική Εργασία

"ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ ΜΕΓΑΛΗΣ ΚΛΙΜΑΚΑΣ ΣΤΟ ΤΟΜΕΑ ΤΗΣ ΥΓΕΙΑΣ"

Μεταπτυχιακή φοιτήτρια: Τραχαναδάκη Γλυκερία

Επιβλέπων καθηγητής: Ψάννης Κωνσταντίνος

Θεσσαλονίκη, Νοέμβριος 2020

Περιεχόμενα

Περίληψη

Ενασχόληση με την έννοια των Big Data, των πλεονεκτημάτων που σχετίζονται με την επεξεργασία τους και τις τεχνολογίες των υπολογιστών μέσω των οποίων αποθηκεύονται και γίνονται αντικείμενο επεξεργασίας. Σχολιασμός των τελευταίων νομικών εξελίξεων σε σχέση με το χειρισμό και την προστασία των ηλεκτρονικών δεδομένων στην Ευρωπαϊκή Ένωση, την Ελλάδα, τον Καναδά, τις Ηνωμένες Πολιτείες Αμερικής, τη Γερμανία και την Ιαπωνία. Ειδική αναφορά στο Γενικό Κανονισμό Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR) και αναφορά στους συγκεκριμένους νόμους κρατών-μελών της Ευρωπαϊκής Ένωσης. Πραγματοποίηση έρευνας, μέσω αυτοσυμπληρούμενων ερωτηματολογίων, με δείγμα συμμετεχόντων νυν και πρώην εργαζόμενους σε χώρους υγείας (με υγειονομικές και διοικητικές ειδικότητες).

Λέξεις Κλειδιά

Big Data, ασφάλεια, ιδιωτικότητα, υγεία, GDPR

Εισαγωγή

Τα τελευταία χρόνια, ο όγκος των δεδομένων που παράγονται και χρησιμοποιούνται σε όλους τους ερευνητικούς, εμπορικούς, κοινωνικούς και τεχνολογικούς τομείς έχει αυξηθεί σημαντικά. Μόνο για το 2018 οι εκτιμήσεις αναφέρουν ότι καθημερινά παράγονται 2,5 πεντάκις εκατομμύρια bytes ανά άνθρωπο ως αποτέλεσμα της ψηφιακής του δραστηριότητας (Social Media Today, 2018). Μάλιστα ο αριθμός αυτός διπλασιάζεται κάθε χρόνο, με αποτέλεσμα η συσσώρευση παλαιών και νέων δεδομένων να φτάνει σε πολύ υψηλά επίπεδα. Αυτά τα μεγέθη είναι ενδεικτικά της τεράστιας ψηφιακής έκρηξης δεδομένων που πραγματοποιείται τα τελευταία χρόνια και συνεχίζει με εκθετικούς ρυθμούς. Πλέον χρειαζόμαστε τεχνολογίες οι οποίες θα μπορούν να επεξεργάζονται δεδομένα σε μεγάλη κλίμακα, παρέχοντας επιπρόσθετα εξελιγμένες υπηρεσίες οι οποίες είναι απαραίτητες για τον όγκο και τη δομή των δεδομένων αυτών. Ο συνδυασμός των τεχνολογιών αυτών έχει επιφέρει την τεχνολογική εξέλιξη που ονομάζεται δεδομένα μεγάλης κλίμακας - Big Data. Η χρήση των Big Data είναι διαφορετική από την επεξεργασία παραδοσιακών δομών δεδομένων λόγω της αδόμητης μορφής τους αλλά και τις ταυτόχρονης απαίτησης για επεξεργασία πραγματικού χρόνου. Επομένως μαζί με τη συλλογή και αποθήκευση Big Data, έχουν πραγματοποιηθεί έρευνες στον τομέα της αναλυτικής, η οποία επιτρέπει την καλύτερη κατανόηση των συλλεχθέντων δεδομένων, τον εντοπισμό κρυμμένων παραμέτρων και την εφαρμογή της παραχθείσας γνώσης σε διαδικασίες που σχετίζονται με τα δεδομένα αυτά (Chen et al., 2014).

Η χρήση των Big Data από πολύ νωρίς έχει επιδείξει σημαντικά οικονομικά οφέλη στους συμμετέχοντες φορείς ή επιχειρήσεις. Έρευνες (Manyika et al., 2011) έχουν δείξει ότι τα big data μπορούν να δημιουργήσουν υπεραξία σε κρίσιμους τομείς μιας χώρας όπως η υγειονομική περίθαλψη, ο δημόσιος τομέας και η οργάνωσή του, η βιομηχανία και το λιανικό εμπόριο. Ενδεικτική της δυναμικής των Big Data είναι η ετήσια έκθεση της Finances Online για τα Big Data, όπου και για το 2019 αναφέρει ότι τα άμεσα οικονομικά οφέλη από τη χρήση των Big Data μέσω κυρίως της πώλησης και εγκατάστασης συσκευών του Διαδικτύου Πραγμάτων εκτιμάται στο 1 τρις δολάρια

(Finances Online, 2020), ώστε όσες εταιρείες δραστηριοποιούνται στον χώρο της αναλυτικής Big Data να αναμένουν σημαντικά οικονομικά οφέλη και νέες ευκαιρίες εμπορικής εξέλιξης. Το παράδειγμα της Αμερικάνικης εταιρείας Netflix, της μεγαλύτερης εταιρείας παροχής ψυχαγωγικού υλικού μέσω διαδικτύου, αναφέρει ότι μέσω της ανάλυσης των επιλογών και γενικότερα της συμπεριφοράς των χρηστών η εταιρεία υλοποίησε βέλτιστους αλγορίθμους συστάσεων με αποτέλεσμα οι χρήστες να είναι ικανοποιημένοι από το προϊόν που τους παρέχεται ενώ η όλη διαδικασία εκτιμάται ότι έχει δημιουργήσει κέρδη 1 δις δολάρια.

Τα δεδομένα μεγάλης κλίμακας δεν αποτελούν μια ξεχωριστή τεχνολογία. Αντιθέτως αποτελούν το συνδυασμό εξελίξεων στη τεχνολογία που συνέβησαν τις τελευταίες δεκαετίες. Οι δυο σημαντικότερες τεχνολογικές εξελίξεις των τελευταίων ετών που συνδέονται με τα Big Data είναι η Νεφοϋπολογιστική και το Διαδίκτυο Πραγμάτων. Οι συνεχώς αυξανόμενοι ρυθμοί αύξησης του μεγέθους, της πολυπλοκότητας αλλά και των απαιτήσεων που προκύπτουν από τη χρήση των Big Data επιφέρουν μερικές σημαντικές προκλήσεις. Εκτός από την αποθήκευση ενός τόσο μεγάλου όγκου δεδομένων, υπάρχουν πολλές ακόμη προκλήσεις που πρέπει να αντιμετωπιστούν, όπως η αναπαράσταση δεδομένων, ο κύκλος ζωής δεδομένων, ο μηχανισμός ανάλυσης, θέματα εμπιστευτικότητας δεδομένων, η διαχείριση ενέργειας, η επεκτασιμότητα και η συνεργασία των εμπλεκόμενων οντοτήτων. Ο κύκλος ζωής των Big Data περιλαμβάνει τα στάδια της παραγωγής, της συλλογής και της ανάλυσης των δεδομένων.

Τα Big Data στον τομέα της υγείας αποτελούνται από σετ δεδομένων τα οποία είναι πολύ μεγάλα, παράγονται με υψηλούς ρυθμούς και είναι πολύ περίπλοκα ώστε να είναι δυνατή η επεξεργασία και ερμηνεία τους από τους πάροχους υγειονομικής με τα υπάρχοντα εργαλεία και τις υφιστάμενες πλατφόρμες. Οι συνεχείς προσπάθειες των υπηρεσιών υγείας των χωρών να είναι πιο αποτελεσματικές και η υγειονομική περίθαλψη πιο βιώσιμη έχουν επιτρέψει και ενθαρρύνει αυτή τη ραγδαία αύξηση του όγκου των Big Data σχετικών με την υγεία. Η εκτίμηση είναι ότι σύντομα σε χώρες με μεγάλους πληθυσμούς θα αποθηκεύονται δεδομένα επιπέδου zettabyte (10^{21}) και yottabyte (10^{24}) (Cottle et al., 2013). Καθώς ο σύγχρονος ανεπτυγμένος κόσμος γερνάει είναι πλέον

επιτακτική η ανάγκη της μετατόπισης της παροχής υπηρεσιών υγείας από την περίθαλψη στην έγκαιρη πρόληψη και παρέμβαση (Andreu-Perez et al., 2015). Αυτή η τάση ενισχύεται και από το γεγονός ότι τα δεδομένα μεγάλης κλίμακας που δημιουργούνται στον τομέα της υγείας αυξάνονται συνεχώς, ειδικά με τη ραγδαία αύξηση σε συσκευές φροντίδας και παρακολούθησης της υγείας ασθενών, συμπεριλαμβανομένων των φορετών συσκευών (wearables).

Ένα από τα βασικά συστατικά των Big Data για την υγεία είναι τα ηλεκτρονικά αρχεία υγείας για ασθενείς που περιλαμβάνουν πληροφορίες που σχετίζονται με το παρελθόν, το παρόν ή το μέλλον της σωματικής ή ψυχικής τους υγείας και χρησιμοποιούνται με πρωταρχικό σκοπό την βελτιστοποιημένη παροχή υπηρεσιών υγείας. Τα αρχεία αυτά έχουν εισάγει πολλά πλεονεκτήματα για τον χειρισμό δεδομένων σχετικά με την υγειονομική περίθαλψη καθώς οι επαγγελματίες υγείας έχουν καλύτερη πρόσβαση σε ολόκληρο το ιατρικό ιστορικό ενός ασθενούς, πραγματοποιείται σημαντική μείωση περιττών εξόδων, υπάρχει η δυνατότητα άμεσης συσχέτισης με τη διαδικασία της ιατροφαρμακευτικής ασφάλισης ασθενών, ενώ η χρήση τους από οργανισμούς ή κρατικές υπηρεσίες επιτρέπει την έγκαιρη αναφορά βασικών δεικτών ποιότητας υγειονομικής περίθαλψης.

Παραδοσιακά, η προστασία δεδομένων απαιτεί την εξασφάλιση τριών κύριων ιδιοτήτων ασφαλείας, εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (Lupton, 2015) όπου η εμπιστευτικότητα αναφέρεται στην προστασία δεδομένων από μη εξουσιοδοτημένες προσβάσεις, η ακεραιότητα ασχολείται με την προστασία δεδομένων από μη εξουσιοδοτημένες τροποποιήσεις και η διαθεσιμότητα διασφαλίζει ότι τα δεδομένα είναι διαθέσιμα σε εξουσιοδοτημένους χρήστες. Αυτές οι τρεις απαιτήσεις εξακολουθούν να είναι πολύ κρίσιμες σήμερα και η εκπλήρωσή τους είναι ακόμα πιο δύσκολη, καθώς οι επιθέσεις δεδομένων είναι πιο περίπλοκες και η έκταση της επίθεσης σε δεδομένα έχει διογκωθεί, λόγω της αύξησης των δραστηριοτήτων συλλογής δεδομένων από πολλές διαφορετικές πηγές και της κοινής χρήσης δεδομένων (Bertino & Ferrari, 2018).

Εκτός από αυτά τα τρία χαρακτηριστικά, το απόρρητο έχει αναδειχθεί ως μια νέα κρίσιμη απαίτηση για την ασφάλεια των δεδομένων. Η εξάπλωση του Διαδικτύου επέτρεψε τη συλλογή τεράστιων αρχείων πληροφοριών για ανθρώπους που μπορεί να μην γνωρίζουν ακριβώς ποιες πληροφορίες αποθηκεύονται για αυτούς, από ποιον συλλέγονται και ποιος έχει πρόσβαση σε αυτές. Επιπρόσθετα, η ραγδαία εξάπλωση των big data έχει φέρει νέες προκλήσεις σε σχέση με την Ασφάλεια και Ιδιωτικότητα των Δεδομένων. Πλέον είναι αναγκαία η διερεύνηση τεχνολογιών και διαδικασιών που θα χειριστούν αυτόν τον τεράστιο όγκο δεδομένων διατηρώντας τα ασφαλή. Οι τρέχουσες τεχνολογίες για την ασφάλεια δεδομένων δεν είναι αποτελεσματικές κυρίως από πλευράς απόδοσης σε σχέση με την ταχύτητα επεξεργασίας, ειδικά όταν εφαρμόζονται σε τεράστιες ποσότητες δεδομένων.

Οι οργανισμοί υγειονομικής περίθαλψης αποθηκεύουν, συντηρούν και μεταδίδουν τεράστιες ποσότητες δεδομένων για να υποστηρίξουν την παροχή αποτελεσματικής και σωστής φροντίδας υγείας. Η ασφάλεια όμως αυτών των δεδομένων έχει θέσει σημαντικές προκλήσεις εδώ και χρόνια. Ειδικότερα ο κλάδος της υγειονομικής περίθαλψης είναι ένας από τους πιο ευάλωτους σε παραβιάσεις δεδομένων. Στην πράξη, οι κακόβουλοι εισβολείς συχνά χρησιμοποιούν μεθόδους και διαδικασίες εξόρυξης δεδομένων για να εντοπίσουν ευαίσθητα δεδομένα τα οποία στη συνέχεια δημοσιοποιούν ή χρησιμοποιούν για προσωπικό όφελος. Ως αποτέλεσμα, είναι κρίσιμο οι οργανισμοί να εφαρμόζουν λύσεις ασφάλειας δεδομένων υγειονομικής περίθαλψης που θα προστατεύουν αποτελεσματικά τα περιουσιακά στοιχεία τους, ενώ ταυτόχρονα θα ικανοποιούνται οι απαιτήσεις για υπηρεσίες υγειονομικής περίθαλψης.

Οι συγγραφείς (Knoppers & Thorogood, 2017) αναφέρονται στη συζήτηση για τους κινδύνους από την κακή χρήση των Big Data (ειδικότερα στην υγεία) και πρεσβεύουν ότι το βάρος της συζήτησης θα έπρεπε να πέφτει κυρίως στο δικαίωμα όλων «να συμμετάσχουν στην επιστημονική πρόοδο και τα οφέλη της». Αυτό το δικαίωμα αναφέρουν ότι έχει τις ρίζες του στην Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων του 1948 και έγινε νομικά δεσμευτικό βάσει του Διεθνούς Συμφώνου για τα Οικονομικά, Κοινωνικά και Πολιτιστικά Δικαιώματα του 1966, το οποίο υπογράφηκε και επικυρώθηκε από 165 χώρες. Λόγω του status ως ανθρώπινο δικαίωμα που

θεσμοθετήθηκε από το διεθνές δίκαιο, το «δικαίωμα στην επιστήμη» έχει καθολική ισχύ και ξεπερνάει τα στεγανά της «βιοηθικής», επιβάλλοντας από τα κράτη να αναλάβουν θετικά σχετικά καθήκοντα.

Επιδιώκοντας την επίλυση των ανωτέρω ζητημάτων, η Ευρωπαϊκή Ένωση εξέδωσε το Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), ο οποίος εφαρμόστηκε σε όλα τα κράτη μέλη της ΕΕ από τις 25 Μαΐου 2018 και αποτελεί ορόσημο στην εξέλιξη του ευρωπαϊκού πλαισίου προστασίας της ιδιωτικότητας (European Law, 2016). Ο κανονισμός αυτός έχει ευρύ παγκόσμιο αντίκτυπο, καθοδηγούμενος από μια φιλοσοφική προσέγγιση στην προστασία των δεδομένων, βασισμένη στην έννοια της ιδιωτικής ζωής ως θεμελιώδους ανθρώπινου δικαιώματος (όπως κατοχυρώνεται στον Χάρτη των Δικαιωμάτων της ΕΕ). Ο νέος νόμος καλύπτει τα προσωπικά δεδομένα όλων των κατοίκων της ΕΕ, ανεξάρτητα από την τοποθεσία που γίνεται η επεξεργασία. Τα προσωπικά δεδομένα είναι πληροφορίες που, άμεσα ή έμμεσα, μπορούν να προσδιορίσουν ένα άτομο και συγκεκριμένα περιλαμβάνουν διαδικτυακά αναγνωριστικά όπως διευθύνσεις IP, cookies και ψηφιακά δακτυλικά αποτυπώματα και δεδομένα τοποθεσίας που θα μπορούσαν να προσδιορίσουν ένα άτομο. Το GDPR διέπεται από αρχές (περιορισμός σκοπού, ελαχιστοποίηση δεδομένων, ακρίβεια,ακεραιότητα), αλλά η προστασία δεδομένων βρίσκεται στον πυρήνα της ουσίας του GDPR.

Απαντώντας στις προκλήσεις της εποχής αναφορικά με την ασφάλεια και ιδιωτικότητα στην εποχή των Big Data, η παρούσα διπλωματική εργασία καλείται να αναλύσει τον τρόπο με τον οποίο καλύπτονται αυτές οι απαιτήσεις σε δεδομένα υγείας. Αφού αναλυθούν οι όροι που αναφέρθηκαν προηγουμένως και συσχετιστούν με τις αντίστοιχες τεχνολογίες, γίνεται μια περιεκτική καταγραφή της υφιστάμενης νομοθεσίας σε αντιπροσωπευτικές χώρες (Ελλάδα, Γερμανία, ΗΠΑ, Καναδάς και Ιαπωνία). Γίνεται ιδιαίτερη αναφορά στους νόμους περί προστασίας των προσωπικών δεδομένων και ειδικά όταν τα δεδομένα αυτά προέρχονται από τον τομέα της υγειονομικής περίθαλψης. Επιπρόσθετα, γίνεται αναφορά και στην εφαρμογή των νόμων στα νοσηλευτικά ιδρύματα των χωρών αυτών.

Το δεύτερος σκέλος της διπλωματικής εργασίας καταγράφει την πραγματοποίηση μιας έρευνας η οποία πραγματοποιήθηκε σε νυν και πρώην εργαζόμενους στο χώρο της υγείας (με υγειονομικές και διοικητικές ειδικότητες) στην Ελλάδα, στον Καναδά και στη Γερμανία. Η έρευνα πραγματοποιήθηκε με αυτοσυμπληρούμενα ερωτηματολόγια μέσω της ηλεκτρονικής πλατφόρμας Google Forms. Το ερωτηματολόγιο έχει 2 μέρη: το πρώτο μέρος περιλαμβάνει τα δημογραφικά στοιχεία ενώ το δεύτερο μέρος ερώτηση σχετικά με την ασφάλεια των ηλεκτρονικών δεδομένων σε επαγγελματικούς χώρους που σχετίζονται με την υγεία.

Ενότητα 1: Θεωρητικό Υπόβαθρο

1.1 Δεδομένα μεγάλης κλίμακας

Τα τελευταία χρόνια, ο όγκος των δεδομένων που παράγονται και χρησιμοποιούνται σε διάφορους τομείς έχει γιγαντωθεί. Οι ρυθμοί αύξησης των δεδομένων προσεγγίζουν τους ρυθμούς εξέλιξης της υπολογιστικής ισχύος των προηγούμενων δεκαετιών, όπου και είχαμε διπλασιασμό περίπου κάθε 2 χρόνια, σύμφωνα με μια έρευνα της IDC (EMC, 2014). Εκτιμάται ότι το 2018 καθημερινά παράγονταν δεδομένα μεγέθους 2,5 πεντάκις εκατομμύρια bytes ανά άνθρωπο (Social Media Today, 2018). Αυτά τα μεγέθη είναι ενδεικτικά της τεράστιας ψηφιακής έκρηξης δεδομένων που πραγματοποιείται τα τελευταία χρόνια και συνεχίζει με εκθετικούς ρυθμούς. Η χρήση δεδομένων μεγάλης κλίμακας διαφέρει από την επεξεργασία παραδοσιακών δεδομένων, καθώς συνήθως τα δεδομένα είναι μη δομημένα και απαιτούν επεξεργασία πραγματικού χρόνου. Η αναλυτική δεδομένων μεγάλης κλίμακας έχει επιτρέψει την καλύτερη κατανόηση και τον εντοπισμό κρυμμένων παραμέτρων σε σχέση με τις διαδικασίες που παράγουν αυτά τα δεδομένα (Chen et al., 2014).

1.1.1 Ορισμός και χαρακτηριστικά

Ο ακριβής ορισμός για τα δεδομένα μεγάλης κλίμακας (Big Data) δεν έχει ακόμα καθοριστεί. Παρά την αναγνωρισμένη αξία τους στη σύγχρονη ψηφιακή εποχή και τις πολλαπλές τεχνολογικές και οικονομικές δυνατότητες αξιοποίησης, οι διάφοροι οργανισμοί και εταιρείες που εμπλέκονται, ορίζουν τα Big Data με βάση τη δική τους οπτική. Ένας πρώτος ορισμός δόθηκε το 2005 και αναφερόταν σε δεδομένα τα οποία είναι αδύνατον να τα διαχειριστούμε και να επεξεργαστούμε με παραδοσιακές τεχνικές επεξεργασίας δεδομένων, εξαιτίας του μεγέθους και της πολυπλοκότητάς τους (Toshniwal et al., 2015). Η κοινότητα του Apache Hadoop το 2010, όρισε τα Big Data ως «σύνολα δεδομένων τα οποία δεν μπορούμε να συλλέξουμε, διαχειριστούμε και επεξεργαστούμε από κανονικούς ηλεκτρονικούς υπολογιστές εντός ενός αποδεκτού πλαισίου». Με βάση αυτό τον ορισμό, τα Big Data τοποθετήθηκαν από την McKinsey & Company, μια εταιρεία συμβουλευτικής στο ανώτερο επίπεδο καινοτομίας και έρευνας

και συνδέθηκαν με τις τεχνολογικές εξελίξεις στον τομέα της Πληροφορικής. Στην ίδια έκθεση προσδιόρισαν ότι το μέγεθος δεν είναι το μοναδικό κριτήριο για τα Big Data, αλλά και η συσχέτισή τους με τον τομέα στον οποίο παράγονται καθώς έτσι αλλάζει τόσο η πολυπλοκότητα όσο και οι επεξεργαστικές ανάγκες (Manyika et al., 2011).

Πριν την καθιέρωση του όρου big data, ο Doug Laney είχε διατυπώσει σε ένα άρθρο για τις ιδιαίτερες απαιτήσεις των σύγχρονων, για την εποχή του, δεδομένων σε σχέση με τα 3 Vs όπως καθιερώθηκε να αναφέρονται: Volume (Όγκος), Velocity (Ταχύτητα), Variety (Ποικιλία). Ο όγκος αναφέρεται στο μέγεθος των παραγόμενων δεδομένων με ιδιαίτερη αναφορά στη δυνατότητα κλιμάκωσης, η ταχύτητα αναφέρεται στη επίκαιρη επεξεργασία των μεγάλων δεδομένων ώστε η συλλογή και ανάλυση δεδομένων να διεξάγεται γρήγορα και έγκαιρα για να αξιοποιείται στο μέγιστο η εμπορική αξία τους, ενώ τέλος η ποικιλία αναφέρεται στις πολλαπλές αναπαραστάσεις και τις διαφορετικές πολυπλοκότητες δεδομένων που μπορεί να περιλαμβάνουν τόσο αδόμητα ή ημι-δομημένα δεδομένα όπως βίντεο, εικόνες, κείμενο, όσο και παραδοσιακά δομημένα δεδομένα (Laney, 2001). Πολλές εταιρείες οικειοποιήθηκαν το μοντέλο 3Vs, μεταξύ των οποίων και οι Gartner, IBM, Microsoft, οι οποίες νωρίς προσδιόρισαν την αξία της επεξεργασίας δεδομένων μεγάλης κλίμακας.

Η IDC επέκτεινε το μοντέλο των 3Vs το 2011, προσθέτοντας μια ακόμη παράμετρο Value (Αξία) και δίνοντας τον ορισμό ότι «οι τεχνολογίες big data αποτελούν μια νέα γενιά τεχνολογιών και αρχιτεκτονικών οι οποίες σχεδιάζονται με σκοπό την αποκομιδή οικονομικών οφελών σε πολύ μεγάλες ποσότητες δεδομένων, επιτρέποντας συλλογή, ανακάλυψη και ανάλυση υψηλής ταχύτητας». Η προσθήκη της Αξίας, σε αντιπαραβολή μάλιστα με τη χαμηλή πυκνότητα που συχνά περιγράφει τα Big Data, επέτρεψε τη συσχέτιση της ανάλυσης των δεδομένων μεγάλης κλίμακας με οικονομικούς και βιομηχανικούς τομείς. Έτσι η αληθινή πρόκληση των Big Data πλέον θεωρήθηκε ότι είναι η αναζήτηση και ο εντοπισμός της κρυμμένης αξίας μέσω διορατικότητας (insight) σε δεδομένα μεγάλης κλίμακας, πολλαπλών τύπων και γρήγορης δημιουργίας.

Η τάση για προσθήκη περισσότερων Vs συνεχίστηκε, ώστε να περιγραφούν πληρέστερα τα ιδιαίτερα χαρακτηριστικά των Big Data. Έτσι οι συγγραφείς του (Andreu-

Perez et al., 2015) επεκτείνουν το μοντέλο σε 6 Vs, προσθέτοντας το Veracity (Αξιοπιστία), το οποίο υποθέτει ότι τα δεδομένα συνήθως είναι αναξιόπιστα οπότε οφείλει η ανάλυση να το λάβει υπόψη και το Variability (Μεταβλητότητα), το οποίο αναφέρεται στο μεταβλητό χαρακτήρα των δεδομένων με πιθανές ασυνέπειες οι οποίες εντοπίζονται με τεχνικές όπως "outlier detection". Σύμφωνα με τους (Uddin & Gupta, 2014) προστέθηκαν άλλα δυο Vs, το Volatility, μεταβλητότητα πάλι, αλλά με την έννοια της χρονικότητας όπου τα δεδομένα έχουν παλαιώσει και ίσως πλέον δεν αποδίδουν τη σωστή εικόνα της κατάστασης που περιγράφουν και το Validity (Καταλληλόλητα), το οποίο συσχετίζει τα δεδομένα με τη χρησιμότητά τους στο συγκεκριμένο πρόβλημα στο οποίο εντάσσονται.

Ορισμένοι μελετητές από τις κοινωνικές επιστήμες έχουν απορρίψει τα μοντέλα που στηρίζονται στα χαρακτηριστικά V, επικρίνοντάς το ότι προέρχονται κυρίως από την επιστήμη ανάλυσης δεδομένων και θεωρούνται πολύ τεχνικά. Μεταξύ αυτών, προτάθηκε το μοντέλο Vs να αντικατασταθεί από το μοντέλο με 13 "P χαρακτηριστικά" όπως portentous, perverse, personal, political, predictive κ.α. (Lupton, 2015). Εντούτοις και αυτό το μοντέλο δέχτηκε κριτική από τους Kitchin & McArdle, καθώς θεωρήθηκε ότι τα περισσότερα χαρακτηριστικά που έχουν προταθεί αποτελούν περιγραφικές ερμηνείες περιφερειακών ζητημάτων των Big Data ενώ τα ιδιαίτερα οντολογικά χαρακτηριστικά αγνοούνται. Ειδικότερα θεωρούν ότι το μέγεθος και η ποικιλία εξαρτώνται άμεσα τόσο από το πρόβλημα όσο και από τις τεχνολογικές εξελίξεις της εποχής, οπότε δεν μπορούν να θεωρούνται ως κρίσιμα και να αναφέρονται στον ορισμό των Big Data (Kitchin & McArdle, 2016).

Παρόλο που έχει πραγματοποιηθεί εκτενής συζήτηση σχετικά με τον ορισμό των Big Data, η ακαδημαϊκή και επιχειρηματική κοινότητα έχουν εστιάσει κυρίως στο πώς θα συλλεχθούν τα δεδομένα και πώς θα μετατραπούν από απλά «πολλά δεδομένα» σε «δεδομένα μεγάλης κλίμακας» (Favaretto et al., 2020). Τέλος, ο πιο πρόσφατος ορισμός των big data από την Ευρωπαϊκή Επιτροπή εξετάζει το όρο περισσότερο από τη σκοπιά του περιεχομένου αναφέροντας ότι τα Big Data είναι «μεγάλες ποσότητες διαφορετικών τύπων δεδομένων που παράγονται από διάφορους τύπους πηγών, όπως άτομα, μηχανήματα ή αισθητήρες. Αυτά τα δεδομένα περιλαμβάνουν πληροφορίες για το κλίμα,

δορυφορικές εικόνες, ψηφιακές εικόνες και βίντεο ή σήματα GPS. Τα Big Data ενδέχεται να περιλαμβάνουν προσωπικά δεδομένα όπως πληροφορίες που σχετίζονται με ένα άτομο (όνομα, φωτογραφία, διεύθυνση email, στοιχεία τράπεζας, δημοσιεύσεις σε ιστότοπους κοινωνικής δικτύωσης, ιατρικές πληροφορίες ή διεύθυνση IP)» (Commission EU, 2019).

1.1.2 Οικονομική και κοινωνική αξία

Από αρκετά νωρίς (2011) υπήρξαν εκτεταμένες μελέτες σχετικά με τα οικονομικά οφέλη της χρήσης των Big Data. Ο McKinsey (Manyika et al., 2011) παρατήρησε μετά από έρευνα ότι τα big data δημιούργησαν υπεραξία σε τομείς όπως η υγειονομική περίθαλψη των ΗΠΑ, η διοίκηση δημοσίου τομέα της Ευρωπαϊκής Ένωσης, το λιανικό εμπόριο στις ΗΠΑ, η παγκόσμια βιομηχανία κατασκευών και τα παγκόσμια δεδομένα γεωγραφικού στίγματος. Έτσι ερευνώντας αυτούς τους πέντε βασικούς κλάδους που αντιπροσωπεύουν την παγκόσμια οικονομία, η έκθεση του McKinsey επισήμανε ότι τα Big Data μπορούν να δώσουν μεγάλη ώθηση στην οικονομική λειτουργία, να βελτιώσουν την παραγωγικότητα και την ανταγωνιστικότητα των επιχειρήσεων και του δημόσιου τομέα και να δημιουργήσουν τεράστια οφέλη για τους καταναλωτές.

Η Finances Online στην ετήσια έκθεσή της για τα Big Data, αναφέρει το 2019 (Finances Online, 2020) ότι τα άμεσα οικονομικά οφέλη από τη χρήση Big Data μέσω κυρίως των εγκαταστάσεων συσκευών του Διαδικτύου Πραγμάτων (IoT) εκτιμούνται για το 2020 στα 1 τρις δολάρια. Έτσι, εταιρείες οι οποίες στηρίζονται σημαντικά στην αναλυτική των Big Data αναμένεται να έχουν πολύ σημαντικά οφέλη. Συγκεκριμένα η έκθεση χρησιμοποιεί το παράδειγμα της Netflix, της μεγαλύτερης εταιρείας παροχής ψυχαγωγικού υλικού μέσω διαδικτύου, όπου η ανάλυση της συμπεριφοράς των χρηστών και η βελτιστοποίηση στους αλγορίθμους συστάσεων εκτιμάται ότι έχει επιφέρει κέρδη 1 δις δολάρια σε νέους πελάτες ή διατηρώντας τους υφιστάμενους. Γενικά η εκτίμηση της έκθεσης είναι ότι η αύξηση των κερδών σε επιχειρήσεις που εκμεταλλεύονται τα Big Data φτάνει στο 8-10% του κύκλου εργασιών τους. Τέλος, η βιομηχανία των Big Data εκτιμάται στα 119 δις δολάρια για το 2020. Είναι εμφανής η τεράστια οικονομική αξία που επιφέρει η χρήση των Big Data καθώς πλέον οι εταιρείες που δεν εκμεταλλεύονται

την δυναμική τους δεν θα μπορούν να ανταπεξέλθουν στον τομέα δραστηριοποίησής τους.

Η αξία των Big Data δεν περιορίζεται μόνο σε οικονομικά οφέλη. Κατά τη διάρκεια της επιδημίας γρίπης του 2009, η Google άντλησε έγκαιρες πληροφορίες αναλύοντας Big Data, τα οποία παρείχαν πληροφορίες ακόμα πιο σχετικές και πολύτιμες από αυτές που παρέχονταν από κέντρα πρόληψης ασθενειών. Καθώς συχνά οι ασθενείς αργούσαν να επισκεφτούν τα κέντρα υγείας, επεδίωκαν την ενημέρωση μέσω πληροφοριών που παρείχε ο παγκόσμιος ιστός. Η Google μελετώντας και συγκρίνοντας τα δεδομένα αναζήτησης πριν την επιδημία και κατά τη διάρκειά της, διαπίστωσε ότι κατά τη διάρκεια της εξάπλωσης της γρίπης, οι καταχωρήσεις που αναζητήθηκαν στις μηχανές αναζήτησης ήταν διαφορετικές απ' ό,τι συνήθως και οι συχνότητες χρήσης των καταχωρήσεων συσχετίστηκαν με την εξάπλωση της γρίπης τόσο χρονικά όσο και τοπικά. Αυτό επέτρεψε εν μέρει την πρόβλεψη νέων εστιών μόλυνσης και την αποτροπή εξάπλωσης του ιού. Τα αποτελέσματα της δράσης της Google αυτή την περίοδο έχουν δημοσιευτεί στο περιοδικό Nature (Ginsberg et al., 2008).

1.1.3 Τύποι δεδομένων

Παρά τον τεράστιο όγκο δεδομένων που παράγονται σε πολλαπλούς τομείς της οικονομικής, τεχνολογικής και βιομηχανικής λειτουργίας, δεν είναι απαραίτητα όλα τα δεδομένα χρήσιμα για τα Big Data analytics. Ορισμένοι τύποι δεδομένων είναι ιδιαίτερα ώριμοι για ανάλυση (EMC, 2012), όπως:

- Εικόνες από χρήστες. Η εξάπλωση των κοινωνικών δικτύων έχει οδηγήσει σε ένα τεράστιο όγκο εικόνων οι οποίες αναρτούνται στις προσωπικές σελίδες των χρηστών. Καθώς λέμε πολλά για τον εαυτό μας όταν δημοσιεύουμε φωτογραφίες δικές μας ή των φίλων μας, η ενσωμάτωση των Big Data έχει εισαγάγει έναν σημαντικό πολλαπλασιαστή στην πληροφορία που μπορεί να περιέχει μια φωτογραφία. Η χρήση τεχνικών μηχανικής μάθησης έχει επιτρέψει την χρήση εξελιγμένων αλγορίθμων προσθήκης ετικετών, κατηγοριοποίησης εικόνων,

εντοπισμού αντικειμένων και άλλες λειτουργίες είτε σε πραγματικό χρόνο κατά τη λήψη είτε μαζικά αφού συγκεντρωθούν από διάφορους ιστότοπους.

- Ψυχαγωγία και κοινωνικά δίκτυα. Οι τάσεις που προκύπτουν από την ανάλυση συμπεριφοράς μεγάλου όγκου χρηστών μπορούν ευκολότερα να εντοπιστούν με τη χρήση Big Data. Η αναζήτηση της βιομηχανίας ψυχαγωγίας για το επόμενο «next big thing» ξεκινάει πλέον από την ανάλυση Big Data και επιτρέπει να προβλεφθούν νικητές και χαμένοι από την αγορά μετοχών, ακόμα και από εκλογικές διαδικασίες. Αυτή η δυναμική είναι πλέον διαθέσιμη χάρη στο τεράστιο όγκο δεδομένων (big data) που δημοσιεύονται οικειοθελώς από τους χρήστες μέσω των κοινωνικών δικτύων.
- Υγεία και Περίθαλψη. Οι αισθητήρες που μετρούν υγειονομικές παραμέτρους δεν είναι πλέον περιορισμένοι μόνο στα ερευνητικά εργαστήρια αλλά έχουν εγκατασταθεί σε νοσοκομεία και κέντρα υγείας. Μετρώντας και παρακολουθώντας δείκτες υγείας του ασθενή, μπορούν να συσχετίσουν την τρέχουσα κατάστασή του σε σχέση με την πάθηση και να επιτρέψουν την πρόληψη, να παρακολουθήσουν πιθανά ξεσπάσματα εξάπλωσης ιών κ.α. σε πραγματικό χρόνο.

1.1.4 Τεχνολογίες

Τα δεδομένα μεγάλης κλίμακας δεν αποτελούν μια ξεχωριστή τεχνολογία. Αντιθέτως αποτελούν το συνδυασμό εξελίξεων στη τεχνολογία που συνέβησαν τις τελευταίες δεκαετίες. Ειδικότερα τα τελευταία χρόνια, η ραγδαία άνοδος στο ρυθμό δημιουργίας Big Data συνδέεται άμεσα με τις τεχνολογικές εξελίξεις στη Νεφοϋπολογιστική και το Διαδίκτυο Πραγμάτων.

Νεφοϋπολογιστική

Η Νεφοϋπολογιστική (cloud computing) σχετίζεται άμεσα με τα Big Data καθώς αποτελεί το κυριότερο εργαλείο αποθήκευσης και επεξεργασίας τους. Ο κύριος στόχος του cloud computing είναι η χρήση τεράστιων υπολογιστικών και αποθηκευτικών πόρων τους οποίους διαχειρίζεται κεντρικά, έτσι ώστε να παρέχονται υπηρεσίες Big Data με

αξιόπιστη και ικανή υπολογιστική απόδοση. Επομένως, η ανάπτυξη συστημάτων cloud computing προσφέρει λύσεις για αποθήκευση και επεξεργασία δεδομένων μεγάλης κλίμακας. Από την άλλη πλευρά, η ραγδαία αύξηση των δεδομένων μεγάλης κλίμακας επιταχύνει επίσης την ανάπτυξη του cloud computing, δημιουργώντας ένα κύκλο ανατροφοδότησης όπου η μια τεχνολογία ενδυναμώνει την άλλη. Το cloud computing διαθέτει δυο χαρακτηριστικά τα οποία επιτρέπουν την αποτελεσματικότερη χρήση των Big Data: κατανεμημένη αποθήκευση η οποία επιτρέπει την αποθήκευση πολύ μεγάλου όγκου δεδομένων και η παράλληλη υπολογιστική που βελτιώνει την αποτελεσματικότητα απόκτησης και ανάλυσης των δεδομένων αυτών (Yang et al., 2017).

Παρόλο που συχνά συγχέονται ως ίδιες τεχνολογίες, το cloud computing διαφέρει σε σχέση με τα Big Data σε δυο κρίσιμα σημεία (Hashen et al., 2015):

(α) Πρώτον, υπάρχει εννοιολογική διαφοροποίηση. Το cloud computing μεταμορφώνει την IoT αρχιτεκτονική, ενώ τα Big Data επηρεάζουν τη λήψη αποφάσεων για τις επιχειρήσεις. Επίσης, τα Big Data εξαρτώνται από το cloud computing ως τη βασική υποδομή για την ομαλή λειτουργία τους. Θα λέγαμε λοιπόν ότι τα Big Data είναι το περιεχόμενο και το cloud computing είναι το πλαίσιο λειτουργίας του περιεχομένου (Stergiou et al., 2018).

(β) Δεύτερον, τα Big Data και το cloud computing στοχεύουν σε διαφορετικούς πελάτες. Το cloud computing είναι μια τεχνολογία που ενδιαφέρει κυρίως την τεχνική υπηρεσία μιας επιχείρησης ως μια προηγμένη λύση πληροφορικής. Τα Big Data είναι ένα προϊόν που ενδιαφέρει το τμήμα λήψης αποφάσεων (συχνά συνδεόμενο με τον CEO της εταιρείας) όπου και παίρνονται οι αποφάσεις με βάση τις κρυφές αξίες που έχουν εντοπιστεί στα αναλυόμενα δεδομένα. Έτσι το cloud computing, με λειτουργίες παρόμοιες με εκείνες των υπολογιστών και των λειτουργικών συστημάτων, παρέχει πόρους σε επίπεδο συστήματος. Τα Big Data λειτουργούν σε ανώτερο επίπεδο από το cloud computing και παρέχουν λειτουργίες παρόμοιες με αυτές των βάσεων δεδομένων.

Διαδίκτυο Πραγμάτων

Ο όρος Διαδίκτυο Πραγμάτων (Internet of things – IoT) πρωτοπαρουσιάστηκε από τον Kevin Ashton το 1999 (Ashton, 2009). Αν και η αρχική του αναφορά ήταν στο πλαίσιο της διαχείρισης αλυσίδας εφοδιασμού, σύντομα ο ορισμός και η εφαρμογή (σε θεωρητικό επίπεδο) του IoT ενσωμάτωσε μια μεγαλύτερη γκάμα λειτουργιών στην υγεία, τις μεταφορές, τις επιχειρήσεις κοινής ωφέλειας κλπ. Οι συγγραφείς (Sundmaeker et al., 2010) σε μια εκτενή ανάλυση του όρου υπό τις οδηγίες του CERP (Cluster of European Research Projects) αναφέρουν ότι «το Διαδίκτυο Πραγμάτων συνδέει τα αντικείμενα του πραγματικού με τον εικονικό κόσμο, επιτρέποντας έτσι συνδεσιμότητα οποιαδήποτε στιγμή, σε οποιοδήποτε μέρος, για οτιδήποτε αντικείμενο και για οποιονδήποτε χρήστη (anytime, anyplace, anything, anyone). Αναφέρεται σε έναν κόσμο όπου τα φυσικά αντικείμενα και όντα αλληλεπιδρούν με τα εικονικά δεδομένα και περιβάλλοντα στον ίδιο χρόνο και χώρο».

Τα Big Data που δημιουργούνται από το IoT έχουν διαφορετικά χαρακτηριστικά σε σύγκριση με τα υπόλοιπα Big Data κυρίως εξαιτίας των πολλών διαφορετικών τύπων δεδομένων που συλλέγονται, τα οποία χαρακτηρίζονται από υψηλή ετερογένεια, ποικιλία, μη δομημένο χαρακτήρα, θόρυβο και πλεονασμό (redundancy). Ακόμα, η μεγάλη πλειοψηφία των Big Data δεν συνδέεται με IoT εγκαταστάσεις, αλλά αυτό εκτιμάται ότι θα αλλάξει καθώς μέχρι το 2030, το πλήθος των εγκατεστημένων αισθητήρων θα φτάσει το ένα τρισεκατομμύριο με αποτέλεσμα τα δεδομένα IoT που θα παράγονται να είναι περισσότερα από τα υπόλοιπα Big Data που θα παράγονται από άλλου τύπου εγκαταστάσεις (πρόβλεψη της HP (Evans, 2011)). Η Intel (Intel, 2020) επισήμανε ότι τα IoT δεδομένα έχουν τρία χαρακτηριστικά που ανταποκρίνονται στο μοντέλο των big data: (i) μεγάλος αριθμός τερματικών που παράγουν μαζικά δεδομένα (ii) τα IoT είναι συνήθως ημι-δομημένα ή μη δομημένα και (iii) τα IoT δεδομένα είναι χρήσιμα μόνο όταν έχουν αναλυθεί.

Προς το παρόν, η ταχύτητα, αποτελεσματικότητα και αποδοτικότητα στην επεξεργασία δεδομένων που παράγονται από το IoT έχει μείνει πίσω σε σχέση με τη συλλογή δεδομένων, κάτι που ωθεί την εξέλιξη και επέκταση των τεχνολογιών που συνδέονται με τα Big Data ώστε να προωθηθεί συνολικά η ανάπτυξη του IoT. Πλέον, οι εταιρείες που δραστηριοποιούνται στο IoT έχουν αντιληφθεί τη σημασία των Big Data,

καθώς η επιτυχία του IoT εξαρτάται από την αποτελεσματική ενσωμάτωση των Big Data και του cloud computing. Έτσι είναι εμφανές ότι αυτές οι τεχνολογίες αλληλεξαρτώνται και πρέπει να αναπτυχθούν από κοινού: από τη μία, η εκτεταμένη ανάπτυξη του IoT θα οδηγήσει σε υψηλότερους ρυθμούς δημιουργίας δεδομένων τόσο σε ποσότητα όσο και σε τύπο, ενώ από την άλλη πλευρά, η εφαρμογή των Big Data στο IoT θα επιταχύνει την εξέλιξη της έρευνας και την ανάπτυξη επιχειρηματικών μοντέλων για το IoT (Dey et al., 2018).

1.1.5 Προκλήσεις

Οι συνεχώς αυξανόμενοι ρυθμοί αύξησης του μεγέθους, της πολυπλοκότητας αλλά και των απαιτήσεων που προκύπτουν από τη χρήση των Big Data επιφέρουν μερικές σημαντικές προκλήσεις. Οι παραδοσιακές σχεσιακές βάσεις δεδομένων δεν μπορούν να ανταπεξέλθουν στις ιδιαίτερες απαιτήσεις των Big Data σε όγκο αλλά και ταχύτητα επεξεργασίας σε πραγματικό χρόνο. Σύγχρονες τεχνολογίες καλούνται να δώσουν τη λύση με σημαντικότερη αυτών τη Νεφοϋπολογιστική η οποία έχει άρρηκτα συνδεθεί πλέον με τα Big Data. Ταυτόχρονα, μετεξελίξεις των σχεσιακών βάσεων δεδομένων όπως τα κατανεμημένα συστήματα και οι NoSQL ΒΔ, έχουν χρησιμοποιηθεί για τις αποθηκευτικές ανάγκες των εφαρμογών που χρησιμοποιούν Big Data. Εκτός από τις αποθηκευτικές μεθόδους, υπάρχουν πολλές ακόμη προκλήσεις που πρέπει να αντιμετωπιστούν. Παρακάτω συνοψίζονται οι πιο σημαντικές που έχουν καταγραφεί από τη σχετική βιβλιογραφία (Lyko et al., 2016):

- Αναπαράσταση δεδομένων: συνήθως ένα σετ δεδομένων δεν έχει σταθερό τύπο δεδομένων, αλλά διακρίνεται από ετερογένεια τόσο στη δομή όσο και στη σημασία, την οργάνωση και τη προσβασιμότητα. Η αναπαράσταση των δεδομένων οφείλει να μοντελοποιήσει (modeling) τα δεδομένα ώστε να είναι πιο αποτελεσματική η ανάλυση και ερμηνεία τους. Εντούτοις, η αναπαράσταση δεν θα πρέπει να αλλοιώνει τα αρχικά χαρακτηριστικά, τα οποία συχνά διαθέτουν κρυφές παραμέτρους που πιθανόν να καταστραφούν κατά τη μοντελοποίηση. Η αποτελεσματική αναπαράσταση δεδομένων αντικατοπτρίζει τη δομή, την κλάση

και τον τύπο των δεδομένων, παρέχοντας και τις κατάλληλες τεχνολογίες ώστε να είναι δυνατή η αποτελεσματική λειτουργία σε διαφορετικά σετ δεδομένων.

- Κύκλος ζωής δεδομένων: Η διάχυτη χρήση αισθητήρων και η διάχυτη υπολογιστική έχουν σημαντικά γρηγορότερους ρυθμούς ανάπτυξης σε σχέση με τις τεχνολογίες αποθήκευσης. Αυτό συχνά οδηγεί τα συστήματα σε αδιέξοδα όπου η αποθήκευση νέων δεδομένων να είναι πλέον αδύνατη ή προβληματική. Κρίνεται λοιπόν αναγκαία η διαδικασία απόρριψης παλαιών δεδομένων τα οποία έχουν χάσει τη χρησιμότητά τους ή έχουν μετατραπεί σε ανωτέρου βαθμού πληροφορίες, ή και απόρριψης νέων δεδομένων τα οποία κρίνονται λιγότερο σημαντικά. Ο κύκλος ζωής δεδομένων αποτελεί μια ουσιαστική διαδικασία η οποία επιτρέπει την τελική βιωσιμότητα ενός συστήματος που διαχειρίζεται Big Data.
- Μηχανισμός ανάλυσης: το σύστημα ανάλυσης Big Data επεξεργάζεται μεγάλες ποσότητες ετερογενών δεδομένων σε περιορισμένο χρόνο. Τα παραδοσιακά συστήματα σχεσιακών ΒΔ δεν μπορούν να ανταπεξέλθουν καθώς ως παραδοσιακά συστήματα προηγούμενων δεκαετιών δεν σχεδιάστηκαν με δυνατότητες επεκτασιμότητας (scalability), οπότε δεν μπορούν να ικανοποιήσουν τις απαιτήσεις απόδοσης. Οι μη σχεσιακές ΒΔ έχουν καλύτερη αποτελεσματικότητα στην επεξεργασία μη δομημένων δεδομένων και άρχισαν να χρησιμοποιούνται σχεδόν αποκλειστικά στην ανάλυση Big Data. Παρόλα αυτά, εξακολουθούν να υπάρχουν ορισμένα προβλήματα των μη σχεσιακών βάσεων δεδομένων σε σχέση με την απόδοσή τους. Η λύση είναι ένα υβριδικό σύστημα μεταξύ των δυο διαφορετικών τεχνολογιών. Για παράδειγμα, ορισμένες επιχειρήσεις έχουν χρησιμοποιήσει μια μικτή αρχιτεκτονική ΒΔ που ενσωματώνει τα πλεονεκτήματα και των δύο τύπων (π.χ. Facebook). Εντούτοις απαιτείται περισσότερη σχετική έρευνα στους μηχανισμούς ανάλυσης και γενικότερα στις βάσεις δεδομένων που θα συνδυαστούν βέλτιστα με τα Big Data.
- Εμπιστευτικότητα δεδομένων: οι περισσότεροι πάροχοι υπηρεσιών Big Data δεν μπορούν για την ώρα να διατηρούν και να αναλύουν πολύ μεγάλα σύνολα δεδομένων λόγω της περιορισμένης χωρητικότητάς των συστημάτων τους. Πρέπει να βασιστούν σε εξωτερικά εργαλεία για την ανάλυση τέτοιων δεδομένων,

κάτι που όμως αυξάνει τους πιθανούς κινδύνους για την ασφάλεια. Για παράδειγμα, ένα σετ/ομάδα δεδομένων που περιλαμβάνει πληροφορίες χρηματικών συναλλαγών μπορεί να περιέχει ευαίσθητες πληροφορίες, όπως αριθμούς πιστωτικών καρτών. Επομένως, η ανάλυση Big Data μπορεί να γίνει από τρίτους μόνο όταν λαμβάνονται κατάλληλα προληπτικά μέτρα για την προστασία τέτοιων ευαίσθητων δεδομένων, ώστε να διασφαλιστεί η ασφάλειά τους.

- Διαχείριση ενέργειας: η κατανάλωση ενέργειας των υπολογιστικών συστημάτων (mainframes) πάντοτε πρόβαλε προκλήσεις τόσο οικονομικές όσο και περιβαλλοντικές. Με την αύξηση του όγκου δεδομένων και των απαιτήσεων που επιφέρουν τα Big Data, η επεξεργασία, η αποθήκευση και η μετάδοση δεδομένων αναπόφευκτα θα καταναλώνουν όλο και περισσότερη ενέργεια. Επομένως, θα πρέπει να δημιουργηθούν μηχανισμοί ελέγχου και διαχείρισης κατανάλωσης σε επίπεδο συστήματος Big Data, ενώ ταυτόχρονα να διασφαλίζεται η δυνατότητα επέκτασης και προσβασιμότητας.
- Επεκτασιμότητα: τα συστήματα ανάλυσης Big Data πρέπει να έχουν τη δυνατότητα να υποστηρίζουν τα υπάρχοντα αλλά και τα μελλοντικά σετ/ομάδες δεδομένων. Επομένως, οι σύγχρονοι αλγόριθμοι αναλυτικής πρέπει να είναι σε θέση να επεξεργάζονται όλο και πιο μεγάλα και πιο περίπλοκα σετ δεδομένων.
- Συνεργασία: η ανάλυση των Big Data είναι ένα διεπιστημονικό πεδίο, το οποίο απαιτεί ερευνητές από διαφορετικούς τομείς να συνεργαστούν για την επίτευξη των προσδοκιών που έχει η παγκόσμια οικονομία από τα Big Data. Κρίνεται λοιπόν αναγκαία η δημιουργία ολοκληρωμένων αρχιτεκτονικών δικτύων τα οποία να είναι διαθέσιμα σε επιστήμονες και μηχανικούς από διάφορους τομείς, οι οποίοι θα αξιοποιούν την εμπειρία τους για τη συνεργατική ανάλυση Big Data και τον αποτελεσματικό εντοπισμό των κρυμμένων αξιών στα δεδομένα .

1.1.6 Κύκλος ζωής Big Data

<u>Παραγωγή δεδομένων</u>

Η παραγωγή δεδομένων είναι το πρώτο βήμα του κύκλου ζωής των Big Data. Αν λάβουμε υπόψη τα δεδομένα Διαδικτύου, παράγονται ένας τεράστιος αριθμός από bytes τα οποία αφορούν καταχωρήσεις αναζήτησης, δημοσιεύσεις σε φόρουμ και κοινωνικά δίκτυα, εγγραφές συνομιλίας, μηνύματα σε microblog πλατφόρμες και σύγχρονες πλατφόρμες συζητήσεων κ.α. Αυτά τα δεδομένα σχετίζονται στενά με την καθημερινότητα των ανθρώπων κληρονομώντας χαρακτηριστικά όπως υψηλή αξία (συχνά κρυμμένη) και χαμηλή πυκνότητα. Τέτοια δεδομένα Διαδικτύου μπορεί να είναι λιγότερο χρήσιμα αν αντιμετωπιστούν ξεχωριστά, αλλά μέσω Big Data αναλυτικής όπου συσχετίζονται μεγάλες ποσότητες δεδομένων μεταξύ τους, είναι δυνατόν να εντοπιστούν χρήσιμες πληροφορίες όπως συνήθειες και χόμπι χρηστών ή και να προβλεφθούν οι συμπεριφορές και οι συναισθηματικές διαθέσεις τους (Lyko et al., 2016).

Επιπλέον, σετ δεδομένων που δημιουργούνται από κατανεμημένες πηγές δεδομένων είναι πιο μεγάλης κλίμακας, με μεγάλη πολυπλοκότητα και διαφορετικούς τύπους. Τέτοιου είδους δεδομένα παράγονται από αισθητήρες κάθε είδους, συσκευές οπτικής καταγραφής (βίντεο ή εικόνα) και άλλες πηγές. Για την ώρα, η κύρια πηγή Big Data είναι οι πλατφόρμες επιχειρήσεων, τα εγκατεστημένα IoT συστήματα, η αλληλεπίδραση των απλών χρηστών με μηχανήματα και δεδομένα που παράγονται από επιστημονική έρευνα. Όπως αναφέρθηκε ήδη, ο όγκος και οι απαιτήσεις για επεξεργαστική ισχύ των δεδομένων που παράγονται δεν μπορούν να ικανοποιηθούν από τις υπάρχουσες IoT πλατφόρμες τόσο για αποθήκευση όσο και για επεξεργασία πραγματικού χρόνου (Geng et al., 2019).

Συλλογή δεδομένων

Η δεύτερη φάση του μοντέλου κύκλου ζωής των Big Data είναι η ανάκτηση των δεδομένων, που περιλαμβάνει τη συλλογή, τη μετάδοση και την προεπεξεργασία τους. Κατά τη λήψη Big Data, αφού προηγηθεί η συλλογή των δεδομένων μέσω των κατάλληλων middleware συστημάτων που επιτρέπουν σε συσκευές παραγωγής δεδομένων με ετερογενή πρωτόκολλα επικοινωνίας να συνδέονται στο σύστημα, τα μη επεξεργασμένα δεδομένα αποστέλλονται σε κατάλληλο σύστημα αποθήκευσης για την υποστήριξη πολλαπλών εφαρμογών. Συχνά, τα δεδομένα που παράγονται από

αισθητήρες IoT, αλλά και από άλλες πηγές, περιλαμβάνουν αρκετά μεγάλο ποσοστό περιττής, άχρηστης ή και λανθασμένης πληροφορίας. Η αποστολή όλου του όγκου των συλλεγόμενων δεδομένων στα συστήματα αποθήκευσης υπερφορτώνει την πλατφόρμα με δεδομένα που θα πρέπει να αποσταλούν, αποθηκευτούν και αναλυθούν χωρίς να προσφέρουν επιπλέον πληροφορία. Κρίνεται λοιπόν σκόπιμο να εκτελεστούν εργασίες προεπεξεργασίας στο σημείο συλλογής δεδομένων, με σημαντικότερη αυτών τη συμπίεση η οποία μειώνει τα φαινόμενα πλεονασμού (Rehman et al., 2016).

Ανάλυση δεδομένων

Η ανάλυση των Big Data περιλαμβάνει κυρίως αναλυτικές μεθόδους για παραδοσιακά δεδομένα και δεδομένα μεγάλης κλίμακας, αρχιτεκτονική για Big Data και λογισμικό για εξόρυξη (mining) και ανάλυση Big Data. Η ανάλυση δεδομένων είναι η τελευταία και πιο σημαντική φάση στον κύκλο ζωής των Big Data, με σκοπό την εξαγωγή χρήσιμων τιμών και την παροχή προτάσεων ή αποφάσεων. Ωστόσο, η ανάλυση δεδομένων είναι μια ευρεία περιοχή, η οποία χαρακτηρίζεται από υψηλή πολυπλοκότητα, διαφοροποίηση σε σχέση με το πεδίο ενδιαφέροντος και μεγάλη συσχέτιση με τις τρέχουσες τάσεις της Πληροφορικής γενικά (Manyika et al., 2011). Στη επόμενη παράγραφο παρουσιάζονται συνοπτικά οι κυριότερες μέθοδοι και εργαλεία για ανάλυση Big Data.

Cluster Analysis είναι μια στατιστική μέθοδος για την ομαδοποίηση αντικειμένων, και συγκεκριμένα την ταξινόμηση αντικειμένων σύμφωνα με εντοπισμένα χαρακτηριστικά (features). Το *Factor Analysis* στοχεύει στην περιγραφή της σχέσης μεταξύ πολλών στοιχείων με λίγους μόνο παράγοντες, δηλαδή την ομαδοποίηση πολλών στενά συνδεδεμένων μεταβλητών σε έναν παράγοντα (factor). Το *Regression Analysis* είναι ένα μαθηματικό εργαλείο για την ανακάλυψη συσχετίσεων μεταξύ μιας μεταβλητής και άλλων μεταβλητών. Η *Στατιστική Ανάλυση* βασίζεται στη στατιστική θεωρία, όπου η τυχαιότητα και η αβεβαιότητα μοντελοποιούνται και εφαρμόζεται ευρέως σε τομείς όπως η οικονομία και η ιατρική περίθαλψη. *Αλγόριθμοι Εξόρυξης Δεδομένων*, όπου είναι μια διαδικασία εξαγωγής κρυφών, άγνωστων, αλλά δυνητικά χρήσιμων πληροφοριών και γνώσεων από μαζικά, θορυβώδη, ασαφή και τυχαία δεδομένα (Erl et al., 2016).

Υπάρχουν πολλά εργαλεία για την εξόρυξη και ανάλυση μεγάλων δεδομένων διαθέσιμα τα οποία μπορεί να είναι είτε ένα ακριβό εμπορικό λογισμικό είτε λογισμικό ανοιχτού κώδικα. Παρακάτω αναφέρονται τα δημοφιλέστερα με βάση μια έρευνα που πραγματοποιήθηκε από την KDNuggets (KDnuggets, 2012). Η γλώσσα R είναι μια γλώσσα προγραμματισμού ανοιχτού κώδικα και ταυτόχρονα ένα IDE, το οποίο έχει σχεδιαστεί για εξόρυξη/ανάλυση δεδομένων και οπτικοποίηση. Είναι μια από τις πιο δημοφιλής επιλογές στα Big Data analytics και χάρη στη δημοφιλία της, μεγάλες εταιρείες διαχείρισης δεδομένων όπως η Oracle παρέχουν εργαλεία και προϊόντα αποκλειστικά για την R. Το περιβάλλον υπολογιστικών φύλλων Excel της Microsoft είναι επίσης αρκετά δημοφιλές καθώς διαθέτει ισχυρές βιβλιοθήκες επεξεργασίας δεδομένων και στατιστικής ανάλυσης όπως το Analysis ToolPak και το Solver Add-in. Το Rapidminer είναι ένα λογισμικό ανοικτού κώδικα για εξόρυξη δεδομένων, μηχανική μάθηση και προβλεπτική ανάλυση. Το KNMINE είναι ένα φιλικό προς το χρήστη εργαλείο για ενσωμάτωση, επεξεργασία δεδομένων, ανάλυση και εξόρυξη δεδομένων. Τέλος το Weka είναι ένα δωρεάν λογισμικό ανοιχτού κώδικα με δυνατότητες μηχανικής μάθησης και εξόρυξης δεδομένων γραμμένο στην Java. Το Weka παρέχει λειτουργίες όπως επεξεργασία δεδομένων, επιλογή χαρακτηριστικών, ταξινόμηση, regression, ομαδοποίηση και οπτικοποίηση (Dwivedi et al., 2016).

1.1.7 Εφαρμογές

Μέχρι σήμερα, τα Big Data προέρχονται αλλά και χρησιμοποιούνται κυρίως από επιχειρήσεις. Οι τεχνολογίες BI και OLAP που χρησιμοποιούνταν από στον επιχειρηματικό τομέα κατά κόρον παλαιότερα μπορούν να θεωρηθούν ως πρόγονοι της αναλυτικής των Big Data. Η εφαρμογή των Big Data στις επιχειρήσεις μπορεί να βελτιώσει την αποδοτικότητα και την ανταγωνιστικότητά τους σε πολλές πτυχές. Συγκεκριμένα στο *μάρκετινγκ*, με ανάλυση συσχέτισης Big Δata, οι επιχειρήσεις μπορούν να προβλέψουν με μεγαλύτερη ακρίβεια τη συμπεριφορά των καταναλωτών και να βρουν νέους επιχειρηματικούς τρόπους προσέγγισής τους. Στον *προγραμματισμό πωλήσεων*, οι επιχειρήσεις μπορούν μέσω σύγκρισης δεδομένων μεγάλης κλίμακας να βελτιστοποιήσουν τις τιμές των εμπορευμάτων τους. Σε επίπεδο *λειτουργίας*, οι επιχειρήσεις μπορούν να βελτιώσουν την αποδοτικότητα της λειτουργίας τους, να

βελτιστοποιήσουν την αξιοποίηση του εργατικού δυναμικού, να προβλέψουν με ακρίβεια τις βέλτιστη κατανομή και νέες ανάγκες προσωπικού, να αποφύγουν την υπερβολική παραγωγή και να μειώσουν το κόστος εργασίας. Τέλος, στην *λειτουργία εφοδιασμού* οι επιχειρήσεις έχουν τη δυνατότητα να βελτιστοποιήσουν το απόθεμα, τα logistics, το συντονισμό προμηθευτών κ.α.., ώστε να περιορίσουν το χάσμα μεταξύ προσφοράς και ζήτησης, να ελέγξουν τον προϋπολογισμό και εν τέλει να βελτιώσουν τις υπηρεσίες που παρέχουν (Cuzzocrea et al., 2017).

Το IoT δεν είναι μόνο μια σημαντική πηγή Big Data, αλλά και μία από τις κύριες αγορές σχετικών εφαρμογών. Λόγω της μεγάλης ποικιλίας «πραγμάτων», οι εφαρμογές του IoT εξελίσσονται συνεχώς ενώ η έξυπνη πόλη είναι ένα περιζήτητο πεδίο έρευνας για την εφαρμογή IoT αρχιτεκτονικών (Plageras et al., 2018). Επιπρόσθετα, η υγειονομική περίθαλψη παράγει συνεχώς ιατρικά δεδομένα τα οποία μπορούν να θεωρηθούν Big Data λόγω της πολυπλοκότητας, του μεγάλου όγκου αλλά και τις υψηλής διαφορετικότητας σε τύπο και κατηγορία. Τα Big Data παρέχουν ισχυρές δυνατότητες για αποτελεσματική αποθήκευση, επεξεργασία, αναζήτηση και ανάλυση ιατρικών δεδομένων. Η εφαρμογή των ιατρικών Big Data θα επηρεάσει σε μεγάλο βαθμό τον τομέα της υγείας τόσο σε επίπεδο επιχειρηματικότητας όσο και σε επίπεδο ιατρικής περίθαλψης και αποδοτικότητας (Andreu-Perez et al., 2015).

Τα σύγχρονα κινητά τηλέφωνα και tablets διαθέτουν όλοένα και πιο ισχυρούς επεξεργαστές και πλήθος αισθητήρων με αποτέλεσμα την ανάπτυξη κοινωνικών πρακτικών όπως το crowd sensing. Αυτός ο όρος αναφέρεται στη δυνατότητα ενός μεγάλου πλήθους τελικών χρηστών να χρησιμοποιεί την κινητή του συσκευή ως «αισθητηριακή μονάδα για τη συμμετοχή σε κατανεμημένη δραστηριοποίηση καταγραφής περιβαλλοντικών παραμέτρων, την συλλογή μαζικών δεδομένων, την ανάλυση και διανομή τους». Αυτή η διαδικασία επιτρέπει να ολοκληρωθούν χρονοβόρες και πολύπλοκες εργασίες πολύ γρηγορότερα. Κρίσιμος παράγοντας επιτυχίας του crowd sensing είναι ότι οι συμμετέχοντες δεν χρειάζεται να διαθέτουν ιδιαίτερες δεξιότητες. Ο πληθοπορισμός (Crowdsourcing) που είναι μια μορφή του crowd sensing, έχει εφαρμόστηκε με επιτυχία σε εφαρμογές όπως επισημείωση (tagging) γεωγραφικών

φωτογραφιών, εντοπισμός γεωγραφικής θέσης και πλοήγηση, ανίχνευση πληροφοριών για αστική κυκλοφορία, πρόβλεψη αγοράς μετοχών, εξόρυξη γνώμης κ.α. (Pilloni, 2018).

1.2 Big Data στην Υγεία

1.2.1 Εισαγωγή

Τα Big Data στον τομέα της υγείας αποτελούνται από σετ δεδομένων τα οποία είναι πολύ μεγάλα, παράγονται με υψηλούς ρυθμούς και είναι πολύ περίπλοκα ώστε να είναι δυνατή η επεξεργασία και ερμηνεία τους από τους πάροχους υγειονομικής με υπάρχοντα εργαλεία και υφιστάμενες πλατφόρμες. Η ραγδαία αύξηση του όγκου των Big Data οφείλεται και στη συνεχιζόμενη προσπάθεια να καταστούν οι υπηρεσίες υγείας πιο αποτελεσματικές και βιώσιμες, λαμβάνοντας υπόψη τις απαιτήσεις ενός συνεχώς αυξανόμενου πληθυσμού, ο οποίος ταυτόχρονα στις αναπτυγμένες χώρες γερνάει, καθώς και τη μετατόπιση της παροχής υπηρεσιών υγείας από την περίθαλψη στην έγκαιρη πρόληψη και παρέμβαση (Andreu-Perez et al., 2015).

Τα μεγέθη των Big Data στη υγεία ακολουθούν το ίδιο μοτίβο με αυτό που αναφέρθηκε στην υποενότητα 1.1. Σύντομα αναμένεται να μιλάμε για μεγέθη δεδομένων επιπέδου zettabyte (10^{21}) και yottabyte (10^{24}) ειδικά σε χώρες με μεγάλους πληθυσμούς, συμπεριλαμβανομένων αναδυόμενων οικονομιών, όπως η Κίνα και η Ινδία (Cottle et al., 2013). Αυτή η τάση οφείλεται στο γεγονός ότι δεδομένα μεγάλης κλίμακας που δημιουργούνται στον τομέα της υγείας αυξάνονται συνεχώς, ειδικά με τη ραγδαία αύξηση στη χρήση συσκευών φροντίδας και παρακολούθησης της υγείας ασθενών, συμπεριλαμβανομένων των φορετών συσκευών (wearables). Οι σύγχρονες συσκευές παρέχουν μεταξύ άλλων μετρήσεις γονιδίου, πρωτεϊνών και μεταβολισμού, υπηρεσίες που μέχρι πρόσφατα ήταν ακριβές και περιορίζονταν σε εξειδικευμένα κέντρα. Παράλληλα, στα Big Data σχετικά με την υγεία συμπεριλαμβάνονται και οι μετρήσεις σε περιβαλλοντικοί παράγοντες που κρίνονται σημαντικοί για την υγεία του πληθυσμού και οι οποίοι μπορούν να καταγραφούν από συσκευές πραγματικού χρόνου, παράγοντας μεγάλες ποσότητες επιπλέον δεδομένων.

Η υγειονομική περίθαλψη εφαρμόζεται σε πολλαπλά επίπεδα ανάλογα με τον επείγοντα χαρακτήρα της κατάστασης. Οι επαγγελματίες χωρίζονται σε αυτούς που παρέχουν συμβουλευτικές υπηρεσίες (πρωτοβάθμια περίθαλψη), καθημερινή περίθαλψη που απαιτεί εξειδικευμένους επαγγελματίες (δευτεροβάθμια περίθαλψη), προηγμένη ιατρική περίθαλψη και θεραπεία (τριτοβάθμια περίθαλψη) και σπάνιες διαγνωστικές ή χειρουργικές διαδικασίες (τεταρτοβάθμια περίθαλψη). Σε όλα αυτά τα επίπεδα, οι επαγγελματίες υγείας είναι υπεύθυνοι για την καταγραφή και ερμηνεία πολλών διαφορετικών ειδών πληροφοριών, όπως το ιατρικό ιστορικό του ασθενούς (και σχετική πληροφορία όπως πρότερες διαγνώσεις και συνταγογραφήσεις), ιατρικά και κλινικά δεδομένα (π.χ. εργαστηριακές εξετάσεις) και άλλα προσωπικά ιατρικά δεδομένα (Bates et al., 2014).

1.2.2 Ηλεκτρονικά αρχεία υγείας

Παλαιότερα, η συνήθης πρακτική αποθήκευσης τέτοιων ιατρικών αρχείων για έναν ασθενή ήταν με τη μορφή χειρόγραφων σημειώσεων, ενώ με την έλευση των συστημάτων υπολογιστών και των δυνατοτήτων τους, η ψηφιοποίηση ιατρικών αρχείων στα συστήματα υγειονομικής περίθαλψης είναι πλέον μια τυπική διαδικασία. Το 2003, το Ινστιτούτο Ιατρικής των Εθνικών Ακαδημιών Επιστημών, Μηχανικών και Ιατρικής των ΗΠΑ επέλεξε τον όρο «ηλεκτρονικά αρχεία υγείας» (electronic health records) για να προσδιορίσει τα αρχεία που διατηρούνται για τη βελτίωση του τομέα της υγειονομικής περίθαλψης προς όφελος των ασθενών και της ιατρικής κοινότητας. Τα ηλεκτρονικά αρχεία υγείας (EHR) ορίστηκαν από τον (Reisman, 2017) ως ηλεκτρονικά ιατρικά αρχεία για ασθενείς που περιλαμβάνουν «πληροφορίες που σχετίζονται με το παρελθόν, το παρόν ή το μέλλον της σωματικής ή ψυχικής τους υγείας και χρησιμοποιούνται από συστήματα τα οποία είναι υπεύθυνα για τη συλλογή, μετάδοση, αποθήκευση, ανάκτηση, σύνδεση και επεξεργασία δεδομένων με πρωταρχικό σκοπό τη βελτιστοποιημένη παροχή υπηρεσιών υγείας».

Τα EHR έχουν εισάγει πολλά πλεονεκτήματα για τον χειρισμό δεδομένων σχετικά με την υγειονομική περίθαλψη. Παρακάτω αναφέρονται μερικά από τα πλεονεκτήματα της χρήσης EHR (Dash et al., 2019):

- Οι επαγγελματίες υγείας έχουν καλύτερη πρόσβαση σε ολόκληρο το ιατρικό ιστορικό ενός ασθενούς. Οι πληροφορίες περιλαμβάνουν ιατρικές διαγνώσεις, συνταγές, δεδομένα που σχετίζονται με γνωστές αλλεργίες, δημογραφικά στοιχεία και αποτελέσματα από εργαστηριακές εξετάσεις. Έτσι, η αναγνώριση και η θεραπεία ιατρικών παθήσεων είναι πιο αποτελεσματική και έγκαιρη
- Τα EHR συμβάλλουν στη σημαντική μείωση σε περιττές εξετάσεις, καθυστερήσεις και απώλειες συνταγογραφήσεων λόγω αμφισημίας σε χειρόγραφα ενώ επιτρέπουν καλύτερο συντονισμό μεταξύ των διάφορων πάροχων υγειονομικής περίθαλψης.
- Οι επαγγελματίες υγείας έχουν τη δυνατότητα πρόσβασης σε διαδικτυακές πλατφόρμες με σκοπό να βελτιώσουν τις ιατρικές τους πρακτικές, χρησιμοποιώντας αυτοματοποιημένες διαδικασίες υποδείξεων και υπενθυμίσεων για εμβολιασμούς, μη φυσιολογικά εργαστηριακά αποτελέσματα και άλλες περιοδικές εξετάσεις.
- Δίνεται η δυνατότητα άμεση συσχέτισης με τη διαδικασία της ιατροφαρμακευτικής ασφάλισης ασθενών, περιορίζοντας τη γραφειοκρατία και τις καθυστερήσεις που αυτή επιφέρει. Επίσης, παρέχονται δεδομένα σχετικά με την ποιότητα της περίθαλψης για τους δικαιούχους προγραμμάτων ασφάλισης υγείας με αποτέλεσμα να γίνεται καλύτερος έλεγχος του αυξανόμενου κόστους των παροχών ασφάλισης υγείας.
- Η χρήση των EHR από οργανισμούς ή κρατικές υπηρεσίες επιτρέπει, μέσω ταχύτερης ανάκτησης μαζικών δεδομένων, την έγκαιρη αναφορά βασικών δεικτών ποιότητας υγειονομικής περίθαλψης, βελτιώνοντας έτσι την παρακολούθηση της δημόσιας υγείας και χάρη σε δυνατότητες άμεσου εντοπισμού εστιών μιας νόσου.
- Τέλος, τα EHR (μετά από επεξεργασία ώστε να αφαιρεθούν τα προσωπικά στοιχεία), παρέχουν πρόσβαση σε εκατομμύρια ιατρικές πληροφορίες που σχετίζονται με την υγεία και είναι ζωτικής σημασίας για την έρευνα στον τομέα της υγειονομικής περίθαλψης και πρόληψης.

Η εξόρυξη πληροφορίας από τα EHR αποτελεί ένα πολύτιμο εργαλείο για τη βελτίωση της ιατρικής γνώσης και την υποστήριξη της κλινικής έρευνας, όπως πχ στην ανακάλυψη φαινοτύπων πληροφοριών (Sun et al., 2014). Η εξόρυξη πληροφοριών τοπικού χαρακτήρα που περιλαμβάνονται στα δεδομένα EHR έχει ήδη αποδειχθεί ότι είναι αποτελεσματική στο να απαντήσει ένα ευρύ φάσμα προκλήσεων στην υγειονομική περίθαλψη, όπως διαχείριση ασθενειών (Eriksson et al., 2014), φαρμακευτική πρόνοια (Friedman et al., 2004), μοντέλα προβλέψεων για εκτίμηση υγειονομικών κινδύνων, συστάσεις θεραπειών (Cars et al., 2013), ανακάλυψη συννοσηρότητας (συνύπαρξη νόσων) και υποστήριξη ενσωμάτωσης ασθενών σε νέες κλινικές δοκιμές.

Παρόμοια με τα EHR, τα «electronic medical records" (EMR) αποθηκεύουν τα τυπικά ιατρικά και κλινικά δεδομένα που συλλέγονται από τους ασθενείς. Τα EHRs, τα EMRs, τα προσωπικά αρχεία υγείας (PHR), και πολλά άλλα δεδομένα υγειονομικής περίθαλψης έχουν συλλογικά τη δυνατότητα να βελτιώσουν την ποιότητα και αποτελεσματικότητα των υπηρεσιών και να μειώσουν το κόστος της υγειονομικής περίθαλψης ταυτόχρονα με τη μείωση ιατρικών σφαλμάτων. Τα Big Data στην υγειονομική περίθαλψη περιλαμβάνουν τα δεδομένα που παράγονται από τους ασθενείς ή τους επαγγελματίας (όπως EMR, συνταγές φαρμάκων και αρχεία ασφάλισης), δεδομένα που παράγονται από γονιδιακά πειράματα (όπως γενότυπος, δεδομένα γονιδιακής έκφρασης κ.α.) και άλλα δεδομένα που αποκτήθηκαν από τους αισθητήρες του Διαδικτύου πραγμάτων. Η υιοθέτηση των EHR ήταν αργή στις αρχές του 21ου αιώνα, ωστόσο αυξήθηκε σημαντικά μετά το 2009 (Eriksson et al., 2014).

1.2.3 Big data στη γενετική

Το ανθρώπινο κύτταρο παρουσιάζει μια υψηλή πολυπλοκότητα σε μοριακές συνδέσεις, το οποίο απαιτεί τη συλλογή πολλών δεδομένων σε πολύ χαμηλό επίπεδο ώστε να είναι δυνατή η ανάλυση που θα οδηγήσει στην κατανόηση των διασυνδέσεων μεταξύ των διάφορων συστατικών και συμβάντων. Τα βιολογικά πειράματα παράγουν μεγάλο όγκο δεδομένων καθώς ακριβώς επειδή εξετάζουν ένα οργανισμό στην κυτταρική του δομή και λειτουργία, η καταγραφή όλων των παραμέτρων τελικά προϋποθέτει την ενσωμάτωση Big Data τεχνολογιών ώστε να είναι αποτελεσματική η

συνολική διαδικασία. Χρειάζονται πολλά επιμέρους μικρά πειράματα τα οποία χρησιμεύουν στη δημιουργία ένα ευρύτερου χάρτη για το βιολογικό φαινόμενο υπό εξέταση. Αυτό υποδεικνύει και την ανάγκη για όσο μεγαλύτερο όγκο δεδομένων, καθώς όσο περισσότερα συλλέγονται τόσο πιο πιθανή είναι η αποκρυπτογράφηση και τελικά κατανόηση του εκάστοτε φαινομένου (Xu, 2020).

Πιθανότατα η μεγαλύτερη επανάσταση στο χώρο έχει επέλθει από την εφαρμογή τεχνολογιών όπως η Αλληλουχία DNA Νέας Γενιάς (next generation sequencing – NGS) στην μοριακή βιολογία (Behjati & Tarpey, 2013). Η ενσωμάτωση δεδομένων μεγάλης κλίμακας σε NGS αλγορίθμους προκάλεσε ραγδαία εξέλιξη σε πολύπλοκες έρευνες με αποκορύφωμα την αποκωδικοποίηση του ανθρώπινου γονιδίου. Η χρήση των Big Data ώστε να αντιληφθούμε επιστημονικές αλήθειες οι οποίες ήταν αδύνατο να παρατηρηθούν με μικρότερης εμβέλειας πειράματα έχει δώσει ώθηση στην έναρξη της εποχής των "-omics" (genomics). Πλέον ο ερευνητής δεν περιορίζεται στη μελέτη ενός γονιδίου, αλλά σε όλο το γονιδίωμα ενός οργανισμού. Κάθε ένα από αυτά τα πειράματα παράγει ένα τεράστιο αριθμό από δεδομένα με υψηλή συσχέτιση και πολυπλοκότητα μεταξύ τους. Εντούτοις υπάρχουν ακόμα αρκετές προκλήσεις στο χώρο, καθώς ο μεγάλος όγκος δεδομένων δεν εξασφαλίζει ότι θα είναι εύκολος ο εντοπισμός καινοτόμων «αξιών», οπότε απαιτείται η σύνδεση των Big Data analytics με το σχετικό επιστημονικό υπόβαθρο της γενετικής (Celesti et al., 2017).

Ένα ολόκληρο ανθρώπινο γονιδίωμα που λαμβάνεται με την αλληλουχία νέας γενιάς (NGS) είναι συνήθως 3 GB. Ανάλογα με το μέσο βάθος κάλυψης, αυτό μπορεί να φτάσει μέχρι και τα 200 GB, καθιστώντας το ως το βασικό συστατικό των Big Data στην υγεία. Ωστόσο, μόνο το 0,1% του γονιδιώματος διαφέρει μεταξύ των ανθρώπων, αντιπροσωπεύοντας περίπου 3 εκατομμύρια παραλλαγές. Από άποψη επεξεργασίας και ανάλυσης, τα δεδομένα αυτά μπορούν να θεωρηθούν ως εξαιρετικά συμπιέσιμα. Ωστόσο, στην πράξη, ο συμπιεσμένος γονότυπος δεν χρησιμοποιείται ευρέως, άρα διατηρείται ο μεγάλος όγκος των δεδομένων που παράγονται για αυτή τη διαδικασία. (Wang et al., 2020)

Η αλληλούχιση γονιδιώματος από το NGS είναι σημαντική για τη μελέτη σύνθετων ασθενειών όπως ο καρκίνος. Ένα από τα μακροχρόνια προβλήματα στη θεραπεία του καρκίνου είναι ότι τα φάρμακα συχνά έχουν ετερογενείς αντιδράσεις στη θεραπεία ακόμη και για τον ίδιο τύπο καρκίνου, και ορισμένα φάρμακα παρουσιάζουν σημαντικά αποτελέσματα μόνο σε μικρό αριθμό ασθενών (Wood, 2013). Πρόσφατα, με τη χρήση των Big Data, έχουν δημιουργηθεί μεγάλης κλίμακας προσωπικά δεδομένα γονιδιωματικής και φαρμακο-γονιδιωματικής φύσεως ώστε να επιτραπεί ο εντοπισμός μοτίβων μεμονωμένων ασθενών και να παρασκευαστούν φάρμακα που στοχεύουν σε αυτά τα μοναδικά μοτίβα. Το project Cancer Genome Atlas του NIH έχει καταγράψει τα προσωπικά γονιδιωματικά προφίλ για πάνω από 10.000 άτομα που εμφανίζουν 20 τύπους καρκίνου και ανακάλυψε νέες υποκατηγορίες καρκίνου με βάση αυτά τα προφίλ (Cancer Genome Atlas Network, 2012).

Τα τελευταία χρόνια υπάρχει έντονο ερευνητικό ενδιαφέρον προς αυτή την κατεύθυνση κάτι που είναι εμφανές και από τη μεγάλη αύξηση των σχετικών επιστημονικών εργασιών. Συγκεκριμένα από λιγότερες από 50 ανά έτος πριν το 2012 έχουμε φτάσει στις σχεδόν 350 για το 2018 (Reisman, 2017). Η χρήση των Big Data και η ενσωμάτωση των σχετικών τεχνολογιών έχει εγείρει σημαντικές προσδοκίες για μια επανάσταση στον τομέα της εξατομικευμένης ιατρικής στο εγγύς μέλλον.

1.2.4 IoT στην υγεία

Η βιομηχανία της ιατρικής περίθαλψης δεν έχει επιδείξει γρήγορα αντανακλαστικά στην ενσωμάτωση της επανάστασης που έχουν επιφέρει τα Big Data, καθώς η χρήση τους στον ιατρικό τομέα βρίσκεται ακόμη σε πολύ πρώιμο στάδιο. Για παράδειγμα, τα Big Data από την ιατρική περίθαλψη και από τη βιοϊατρική δεν έχουν ακόμα συγκλίνει σε ένα ενιαίο σύνολο δεδομένων ώστε να ενισχυθεί η περίθαλψη μέσω της μοριακής παθολογίας. Εφόσον πραγματοποιηθεί, μια τέτοια σύγκλιση θα επιτρέψει τη λειτουργία μηχανισμών από την προληπτική βιολογία στην ιατρική περίθαλψη. Επομένως απαιτούνται τεχνολογίες όπως το Διαδίκτυο Πραγμάτων που θα επιτρέψουν αυτή την ομαλή σύνδεση μεταξύ ετερογενών σετ δεδομένων.

Χρησιμοποιώντας το δίκτυο των IoT συσκευών, ένας γιατρός θα μπορεί να μετράει και να παρακολουθεί διάφορες παραμέτρους των ασθενών του, σε διάφορα σημεία όπως το σπίτι ή το γραφείο τους. Έτσι, μέσω έγκαιρης παρέμβασης και θεραπείας, ένας ασθενής μπορεί να μην χρειαστεί νοσηλεία ή ακόμη και να επισκεφθεί το γιατρό με αποτέλεσμα τη σημαντική μείωση του κόστους στα έξοδα περίθαλψης. Μερικά παραδείγματα συσκευών IoT που χρησιμοποιούνται στην υγειονομική περίθαλψη περιλαμβάνουν φορετές συσκευές μέτρησης φυσικής κατάστασης, βιοαισθητήρες, κλινικές συσκευές για την παρακολούθηση ζωτικών σημείων κ.α. παράγοντας μεγάλο αριθμό δεδομένων που σχετίζονται με την υγεία. Εφόσον μπορέσουμε να ενσωματώσουμε αυτά τα δεδομένα με άλλα υπάρχοντα δεδομένα υγειονομικής περίθαλψης όπως τα EMR, μπορούμε να προβλέψουμε την κατάσταση της υγείας ενός ασθενούς και την εξέλιξή του από υπο-κλινική σε παθολογική κατάσταση (Shameer et al., 2017). Σε μεγαλύτερη κλίμακα, τα δεδομένα από τέτοιες συσκευές μπορούν να βοηθήσουν στην παρακολούθηση της υγείας του προσωπικού, στη μοντελοποίηση της εξάπλωσης μιας ασθένειας και στην εξεύρεση τρόπων για τον περιορισμό μιας συγκεκριμένης επιδημίας.

1.2.5 mHealth

Στον σύγχρονο ψηφιακό κόσμο, μια από τις τελευταίες εμμονές των ανθρώπων είναι η παρακολούθηση στατιστικών δεικτών για την υγεία του μέσω ενσωματωμένων αισθητήρων στα κινητά τους τηλέφωνα, ρολόγια, ταμπλέτες ή άλλες φορητές έξυπνες συσκευές. Μέσα σε μια κοινωνία που συνεχώς μετεξελίσσεται σε «κινητή» σε όλες σχεδόν τις πτυχές της καθημερινότητας, η υποδομή υγειονομικής περίθαλψης χρειάζεται αναδιαμόρφωση για να φιλοξενήσει τα δεδομένα αυτά που παράγονται από τις κινητές συσκευές (Moore, 2001). Η πρακτική της ιατρικής περίθαλψης και δημόσιας υγείας χρησιμοποιώντας κινητές συσκευές, έχει ονομαστεί mHealth (mobile Health), και έχει εφαρμογή σε πολλά στάδια της υγειονομικής περίθαλψης ειδικά για χρόνιες ασθένειες, όπως ο διαβήτης και ο καρκίνος (Nasi et al., 2015). Οι οργανισμοί υγειονομικής περίθαλψης χρησιμοποιούν όλο και περισσότερο κινητές υπηρεσίες υγείας και ευεξίας για την εφαρμογή καινοτόμων τρόπων παροχής φροντίδας και συντονισμού της υγείας των πελατών τους. Οι κινητές πλατφόρμες μπορούν να βελτιώσουν την υγειονομική

περίθαλψη επιταχύνοντας τη διαδραστική επικοινωνία μεταξύ ασθενών και παρόχων υγειονομικής περίθαλψης. Έτσι τόσο η Apple (ReseachKit) όσο και η Google (Google Fit) έχουν υλοποιήσει την δική τους διάχυτη πλατφόρμα υγείας για τη υποστήριξη αντίστοιχων εφαρμογών (Apple, 2020). Αυτές οι πλατφόρμες υποστηρίζουν την απρόσκοπτη αλληλεπίδραση με διάφορες εμπορικές συσκευές και ενσωματωμένους αισθητήρες για ενοποίηση δεδομένων. Επίσης, βοηθούν τους γιατρούς να έχουν άμεση πρόσβαση στα συνολικά δεδομένα υγείας ενός ασθενή τους. Τόσο ο χρήστης όσο και ο γιατρός γνωρίζουν την κατάσταση της υγείας του σε πραγματικό χρόνο. Τέλος οι εφαρμογές επιτρέπουν τον σχεδιασμό πλάνου ευεξίας, ενθαρρύνοντας τον υγιή τρόπο ζωής, δίνοντας καθημερινούς στόχους, παροτρύνοντας το χρήστη να συμμετέχει και να επιτυγχάνει τους στόχους αυτούς. Έτσι απλοί χρήστες αλλά και ασθενείς μπορούν έμπρακτα να υποστηρίξουν και παρακολουθήσουν τη δική τους υγεία.

Σύμφωνα με τους συγγραφείς (Andreu-Perez et al., 2015) τρεις παράγοντες συνέβαλαν στην ταχεία εξάπλωση των φορητών συσκευών: αυξημένη επεξεργαστική ισχύς, ταχύτερη ασύρματη επικοινωνία χάρη στις ευρυζωνικές συνδέσεις και βελτιωμένος σχεδιασμός στις συσκευές αισθητήρων. Τα παλαιότερα συστήματα φορετών συσκευών είχαν περιορισμένη συνδεσιμότητα και περιλάμβαναν συνήθως ένα αισθητήρα ενώ είχαν αναπτυχθεί για ερευνητικούς σκοπούς. Τα πιο σύγχρονα συστήματα έχουν διάχυτη συνδεσιμότητα, διαθέτουν πλήθος από αισθητήρες σε ευκολοφόρετες και ευκολόχρηστες συσκευές, με δυνατότητες πολλαπλών τρόπων ανίχνευσης και αναπτύσσονται σε ευρύ φάσμα ιατρικών εφαρμογών (Zheng et al., 2014). Τέλος, οι τεχνολογικές εξελίξεις στην υλοποίηση μικροσκοπικών αισθητήρων, στη μικροηλεκτρονική και στη διαθεσιμότητα ασύρματων δικτύων έχουν βελτιώσει την προσαρμοστικότητα και ευχρηστία των wearables (Rashidi & Mihailidis, 2012).

1.2.5 Κλίμα και big data

Τα κλιματικά δεδομένα τα οποία συνδέονται άμεσα με επιπτώσεις υγείας, όπως υψηλή παρουσία νέφους σε αστικά κέντρα ή θνησιμότητα λόγω παγετού/καύσωνα, αποτελούν μια ακόμα διάσταση Big Data των οποίων η ανάλυση μπορεί να προβλέψει τη δημόσια υγεία. (Kovats & Hajat, 2008). Οι πρόσφατες εξελίξεις στις συσκευές

αισθητηρίων και τα Γεωγραφικά συστήματα πληροφοριών (GIS) επιτρέπουν την συλλογή κλιματικών δεδομένων σε μεγάλη έκταση, με χωρική ανάλυση μέχρι και 500 μέτρα (Friedl et al., 2010). Σε αρκετές έξυπνες πόλεις πλέον, ένα πυκνό πλέγμα από αισθητήρες συλλέγει περιβαλλοντικά δεδομένα τα οποία μετά από επεξεργασία μπορούν να υπολογίζουν τη χωροχρονική μεταβλητότητα επιβλαβών παραμέτρων όπως η τοξικότητα του αέρα (Moltchanov et al., 2015). Η επίτευξη τόσο υψηλών αναλύσεων σε μετρήσεις περιβαλλοντικών και κλιματικών δεδομένων επιτρέπει την αποτελεσματικότερη παρακολούθηση των επιπτώσεων της ρύπανσης στην υγιεινή των αστικών περιοχών. Αυτή η εφαρμογή της τεχνολογίας αισθητήρων αναμένεται να αποτελέσει ένα κρίσιμο πόρο για τη συσχέτιση της επιδημιολογικής ευφυίας με την παρακολούθηση των παθήσεων και επιπτώσεων στις έξυπνες πόλεις του μέλλοντος.

1.2.6 Εφαρμογές

Το IoT αναμένεται να δώσει πρόσβαση σε μια ποικιλία υπηρεσιών υγειονομικής περίθαλψης για ένα ευρύ φάσμα του πληθυσμού, παρέχοντας αυτοματοποιημένη ιατρική περίθαλψη και αποτελεσματική αντίδραση σε καταστάσεις έκτακτης ανάγκης. Οι (Islam et al., 2015) περιγράφουν μια λίστα τέτοιων υπηρεσιών και εφαρμογών:

- Ambient Assisted Living (AAL), μια παραλλαγή του έξυπνου σπιτιού στην Υγεία. Ο κύριος σκοπός είναι να παρέχει έναν ανεξάρτητο τρόπο ζωής για τους ηλικιωμένους και άλλα άτομα, εξασφαλίζοντας μεγαλύτερη αυτονομία και εποπτεία για την ανίχνευση οποιουδήποτε προβλήματος. Δεδομένου ότι το AAL περιορίζεται κυρίως σε έναν συγκεκριμένο χώρο διαβίωσης, η αρχιτεκτονική του συστήματος θα πρέπει να παρέχει τοπικές υπηρεσίες γρήγορα και αποτελεσματικά. Οι παράμετροι περιβάλλοντος είναι διαθέσιμες ανά πάσα στιγμή, από τους αισθητήρες που αναπτύσσονται στο προσωπικό δίκτυο του ασθενή (Body Area Network).
- Παρακολούθηση ιατρικής κατάστασης. Παρόμοια με την AAL, η διαδικασία αυτή περιορίζεται ως εύρος ευθυνών στη συνεχή παρακολούθηση της ιατρικής κατάστασης του ασθενούς. Μεταξύ των πιο συνηθισμένων μετρήσεων είναι: ανίχνευση γλυκόζης, ηλεκτροκαρδιογράφημα, αρτηριακή πίεση, θερμοκρασία

σώματος και κορεσμός οξυγόνου. Οι αισθητήρες στο σώμα του ασθενούς υποδεικνύουν ανωμαλίες που πρέπει να διερευνηθούν μαζί με τη λήψη επιπλέον δεδομένων περιβάλλοντος από τους γύρω αισθητήρες.

- Ανίχνευση πτώσης. Όντας από τις κύριες αιτίες θανάτου άνω των 65 ετών, οι τυχαίες πτώσεις έχουν λάβει αρκετή προσοχή από τους ερευνητές της έξυπνης υγείας. Τα επιταχυνσιόμετρα και τα γυροσκόπια είναι οι πιο συνηθισμένοι αισθητήρες που χρησιμοποιούνται, αλλά ορισμένες μελέτες προτείνουν τη διακριτική χρήση της παρακολούθησης βίντεο (Hansen et al., 2005).
- Δραστηριότητες της καθημερινότητας. Σχετιζόμενη με την ανίχνευση πτώσης, η αναγνώριση της δραστηριότητας είναι πληροφορία πλαισίου (context) υψηλής αξίας χρήσιμη σε όλες τις εφαρμογές υγειονομικής περίθαλψης. Αν και δεν θεωρείται από μόνη της εφαρμογή, αυτή η λειτουργικότητα μπορεί να θεωρηθεί ως αυτόνομη διαδικασία που μπορεί να συνεργαστεί με εφαρμογές υγείας.
- Διαχείριση φαρμάκων. Η μη συμμόρφωση και η παραμέληση της πρόσληψης φαρμάκων είναι συχνά φαινόμενα ειδικά όταν υπάρχουν γνωσιακές αναπηρίες. Η υποδομή IoT μπορεί να παρέχει υπηρεσίες για την αποτροπή τέτοιων φαινομένων, προσθέτοντας κατάλληλους αισθητήρες στη συσκευασία φαρμάκων. Το πλαίσιο είναι αρκετά απλό σε αυτήν την εφαρμογή. Ο ασθενής είτε έχει πάρει το φάρμακό του είτε όχι την προβλεπόμενη ώρα, μια πληροφορία που μπορεί να μεταδοθεί σε ένα προκαθορισμένο υγειονομικό επιμελητή (γιατρό ή νοσηλευτή).

1.3 Ασφάλεια και Big Data

1.3.1 Προστασία Δεδομένων

Παραδοσιακά, η προστασία δεδομένων απαιτεί την εξασφάλιση τριών κύριων ιδιοτήτων ασφαλείας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα (Lupton, 2015), επίσης γνωστή ως τριάδα της CIA. Η εμπιστευτικότητα αναφέρεται στην προστασία δεδομένων από μη εξουσιοδοτημένες προσβάσεις ανάγνωσης, ενώ η ακεραιότητα ασχολείται με την προστασία δεδομένων από μη εξουσιοδοτημένες τροποποιήσεις. Η ακεραιότητα των δεδομένων γενικεύτηκε περαιτέρω στην αξιοπιστία των δεδομένων, η οποία αναφέρεται στη διασφάλιση όχι μόνο ότι τα δεδομένα δεν

τροποποιούνται από μη εξουσιοδοτημένα άτομα, αλλά και ότι τα δεδομένα είναι απαλλαγμένα από σφάλματα, είναι ενημερωμένα και προέρχονται από αξιόπιστες πηγές. Η διασφάλιση της αξιοπιστίας των δεδομένων είναι ένα δύσκολο πρόβλημα που συχνά εξαρτάται από τον τομέα της εφαρμογής. Η λύση του απαιτεί συνδυασμό διαφορετικών τεχνικών, που περιλαμβάνουν (α) κρυπτογραφικές τεχνικές για την ψηφιακή υπογραφή των δεδομένων, (β) τον έλεγχο πρόσβασης δηλαδή ότι μόνο εξουσιοδοτημένα άτομα τροποποιούν τα δεδομένα, (γ) τεχνικές ποιότητας δεδομένων για αυτόματη ανίχνευση και διόρθωση σφαλμάτων δεδομένων (Toshniwal et al., 2015), (δ) τεχνικές προέλευσης για τον προσδιορισμό από ποιες πηγές προέρχονται τα δεδομένα και (ε) τεχνικές για την αξιολόγηση της φήμης των πηγών δεδομένων. Τέλος, η διαθεσιμότητα διασφαλίζει ότι τα δεδομένα είναι διαθέσιμα σε εξουσιοδοτημένους χρήστες. Αυτές οι τρεις απαιτήσεις εξακολουθούν να είναι πολύ κρίσιμες σήμερα και η εκπλήρωσή τους είναι ακόμα πιο δύσκολη, καθώς οι επιθέσεις δεδομένων είναι πιο περίπλοκες και η έκταση της επίθεσης σε δεδομένα έχει διογκωθεί, λόγω της αύξησης των δραστηριοτήτων συλλογής δεδομένων από πολλές διαφορετικές πηγές και της κοινής χρήσης δεδομένων. (Bertino & Ferrari, 2018)

Εκτός από την τριάδα της CIA, το απόρρητο έχει αναδειχθεί ως μια νέα κρίσιμη απαίτηση στη συζήτηση για την ασφάλεια των δεδομένων. Έχουν προταθεί πολλοί ορισμοί της ιδιωτικότητας δεδομένων και η έννοιά της έχει εξελιχθεί με την πάροδο του χρόνου ως αποτέλεσμα της εξέλιξης των μέσων απόκτησης προσωπικών πληροφοριών. Η εμφάνιση και η εξάπλωση του Διαδικτύου και του Παγκόσμιου Ιστού επέτρεψαν τη συλλογή τεράστιων αρχείων πληροφοριών για τα άτομα (π.χ. οικονομικό και πιστωτικό ιστορικό, ιατρικά αρχεία, ιστορικό αγορών, τηλεφωνικές κλήσεις) που μπορεί να μην γνωρίζουν ακριβώς ποιες πληροφορίες αποθηκεύονται για αυτούς, από ποιον συλλέγονται και ποιος έχει πρόσβαση σε αυτές. Σήμερα, ένας από τους πιο δημοφιλείς ορισμούς του απορρήτου των δεδομένων οφείλεται στον Allan Westin που ορίζει το απόρρητο των δεδομένων ως «το δικαίωμα των ατόμων, ομάδων ή ιδρυμάτων να καθορίσουν πότε, πώς και σε ποιο βαθμό οι πληροφορίες σχετικά με αυτούς κοινοποιούνται σε άλλους» (Westin, 1968).

Η ραγδαία εξάπλωση των Big Data έχει φέρει νέες προκλήσεις σε σχέση με την Ασφάλεια και Ιδιωτικότητα των Δεδομένων. Πλέον είναι αναγκαία η διερεύνηση τεχνολογιών και διαδικασιών που θα χειριστούν αυτό τον τεράστιο όγκο δεδομένων διατηρώντας τα ασφαλή. Οι τρέχουσες τεχνολογίες για την ασφάλεια δεδομένων δεν είναι αποτελεσματικές κυρίως από πλευράς απόδοσης σε σχέση με την ταχύτητα επεξεργασίας, ειδικά όταν εφαρμόζονται σε τεράστιες ποσότητες δεδομένων. Οι συγγραφείς (Toshniwal et al., 2015) αξιολογούν τους πιο δημοφιλείς αλγόριθμους για κρυπτογράφηση δεδομένων, συμπεραίνοντας ότι και οι πιο γρήγοροι από αυτούς δεν μπορούν να ξεπεράσουν τα 64.3 MB/sec. Ωστόσο η έλευση των Big Data όπου ο όγκος των δεδομένων μετράται πλέον σε ένα Gigabytes ή και Petabytes, κατέστησε αυτούς τους αλγόριθμους ανεπαρκείς, ειδικά καθώς η επεξεργασία των Big Data συχνά απαιτείται να γίνει σε πραγματικό χρόνο. Επομένως εντοπίζεται η ανάγκη για νέες μεθόδους ασφάλειας δεδομένων και γενικά ταχύτερες τεχνικές κρυπτογράφησης.

Μια άλλη πρόκληση που θέτουν τα Big Data είναι η επεξεργασία ερωτημάτων (queries) σε κρυπτογραφημένα δεδομένα. Συνήθως, η επεξεργασία queries τόσο σε μη δομημένα όσο και σε δομημένα κρυπτογραφημένα δεδομένα απαιτεί πρώτα την αποκρυπτογράφηση των δεδομένων. Όμως λόγω των τεράστιων ποσοτήτων δεδομένων, αυτό μπορεί να απαιτήσει σημαντικό χρόνο και η επεξεργασία ερωτημάτων τελικά να διαρκέσει περισσότερο απ’ ό,τι προβλέπεται από την εκάστοτε εφαρμογή. Σύμφωνα με τους (Toshniwal et al., 2015) γίνεται αναφορά στον παραδοσιακό σχήμα επεξεργασίας ερωτημάτων σε κρυπτογραφημένα δεδομένα όπου (α) παράγεται το ερώτημα, (β) τα δεδομένα αποκρυπτογραφούνται με βάση το δημόσιο κλειδί, (γ) γίνεται επεξεργασία του ερωτήματος και παράγονται τα αποτελέσματα και (δ) τα αποτελέσματα κρυπτογραφούνται πάλι με βάση το δημόσιο κλειδί. Το παραπάνω σχήμα οι συγγραφείς του άρθρου το προσαρμόζουν σε εφαρμογές Big Data προτείνοντας την παρακάτω σειρά ενεργειών: (α) παράγεται το ερώτημα με ενσωματωμένο δημόσιο κλειδί, (β) γίνεται επεξεργασία του ερωτήματος πάνω σε κρυπρογραφημένα δεδομένα, (γ) παράγονται κρυπτογραφημένα αποτελέσματα και (δ) τα αποτελέσματα αποκρυπτογραφούνται από τον ενδιαφερόμενο. Αυτή η πρόταση σχήματος απαιτεί την κρυπτογράφηση και αποκρυπτογράφηση πολύ μικρότερου όγκου δεδομένων, κάτι που σύμφωνα με τους

συγγραφείς μπορεί να την καταστήσει κατάλληλη για περιβάλλοντα που χειρίζονται Big Data.

Όπως αναφέρθηκε, η ενσωμάτωση των Big Data προϋποθέτει την εφαρμογή άλλων σύγχρονων τεχνολογιών όπως το Διαδίκτυο Πραγμάτων και το Cloud Computing. Η σύγκλιση αυτών των δυο τεχνολογιών κρύβει αρκετούς κινδύνους σε θέματα ασφάλειας. Συγκεκριμένα, όταν κρίσιμες εφαρμογές IoT μεταφέρουν της διαδικασίες τους στο νέφος, εγείρονται ανησυχίες σε σχέση με την εμπιστοσύνη που υπάρχει μεταξύ του πάροχου υπηρεσιών νέφους και το αποδέκτη, που συχνά χρησιμοποιεί το IoT για να επεκτείνει τις ίδιες δραστηριότητές και όχι να παρέχει περαιτέρω υπηρεσίες σε πελάτες. Οι ανησυχίες συνδέονται και με την έλλειψη ενημέρωσης σχετικά με τα Service Level Agreements (SLAs) αλλά και με τη φυσική τοποθεσία αποθήκευσης των δεδομένων. Τέλος, η πολλαπλή μίσθωση (multitenancy) σε υπηρεσίες Cloud μπορεί να απαιτήσει συμβιβασμό στην ασφάλεια ή και να οδηγήσει σε διαρροή ευαίσθητων δεδομένων. Οι συγγραφείς της (Intel, 2020) προτείνουν ένα σύστημα ασφαλούς σύγκλισης μεταξύ του Νέφους και των IoT εφαρμογών, τοποθετώντας ανάμεσά τους ένα τείχος ασφαλείας. Συγκεκριμένα, προτείνουν την ενσωμάτωση μιας καινοτόμου πλατφόρμας η οποία θα έχει δυνατότητα κλιμάκωσης για την υποστήριξη υπηρεσιών ασφάλειας και ιδιωτικότητας σε αυξανόμενο αριθμό κόμβων.

1.3.2 Τεχνολογίες Ασφάλειας Big Data στην Υγεία

Οι οργανισμοί υγειονομικής περίθαλψης αποθηκεύουν, συντηρούν και μεταδίδουν τεράστιες ποσότητες δεδομένων για να υποστηρίξουν την παροχή αποτελεσματικής και σωστής φροντίδας υγείας. Η ασφάλεια όμως αυτών των δεδομένων έχει θέσει σημαντικές προκλήσεις εδώ και χρόνια. Ειδικότερα ο κλάδος της υγειονομικής περίθαλψης είναι ένας από τους πιο ευάλωτους σε παραβιάσεις δεδομένων. Στην πράξη, οι κακόβουλοι εισβολείς συχνά χρησιμοποιούν μεθόδους και διαδικασίες εξόρυξης δεδομένων για να εντοπίσουν ευαίσθητα δεδομένα τα οποία στη συνέχεια δημοσιοποιούν ή χρησιμοποιούν για προσωπικό όφελος. Ενώ μάλιστα η εφαρμογή μέτρων ασφαλείας παραμένει μια περίπλοκη διαδικασία, οι κίνδυνοι συνεχώς αυξάνονται καθώς οι τρόποι για να αντιμετωπιστούν τα κενά ασφαλείας γίνονται ολοένα και πιο περίπλοκοι. Ως

αποτέλεσμα, είναι κρίσιμο οι οργανισμοί να εφαρμόζουν λύσεις ασφάλειας δεδομένων υγειονομικής περίθαλψης που θα προστατεύουν αποτελεσματικά τα περιουσιακά στοιχεία τους, ενώ ταυτόχρονα θα ικανοποιούνται οι απαιτήσεις για υπηρεσίες υγειονομικής περίθαλψης. (Abouelmehdi et al., 2017)

Χρησιμοποιούνται διάφορες τεχνολογίες για την προστασία της ασφάλειας και του απορρήτου των δεδομένων υγειονομικής περίθαλψης. Οι πιο ευρέως χρησιμοποιούμενες τεχνολογίες είναι:

Έλεγχος ταυτότητας: Ο έλεγχος ταυτότητας είναι η διαδικασία που αποδεικνύει ή επιβεβαιώνει ότι οι αξιώσεις που γίνονται από χρήστες είναι αυθεντικές. Εξυπηρετεί μια κρίσιμη λειτουργία σε οποιονδήποτε οργανισμό: την εξασφάλιση πρόσβασης σε εταιρικά δίκτυα, με προστασία της ταυτότητας των χρηστών και διασφάλιση ότι ένας χρήστης είναι αυτός που ισχυρίζεται ότι είναι. Τα περισσότερα κρυπτογραφικά πρωτόκολλα περιλαμβάνουν κάποια μορφή ελέγχου ταυτότητας τελικού χρήστη ειδικά για την αποτροπή επιθέσεων (man-in-the-middle - MITM). Για παράδειγμα, το Transport Layer Security (TLS) και ο προκάτοχός του, Secure Sockets Layer (SSL), είναι κρυπτογραφικά πρωτόκολλα που παρέχουν ασφάλεια για επικοινωνίες μέσω δικτύων όπως το Διαδίκτυο. Τα TLS και SSL κρυπτογραφούν τα μέρη των συνδέσεων δικτύου στο επίπεδο μεταφοράς από άκρο σε άκρο. Χρησιμοποιούνται ευρέως σε εφαρμογές όπως περιήγηση στο Web, ηλεκτρονικό ταχυδρομείο, φαξ μέσω Διαδικτύου, ανταλλαγή μηνυμάτων και voice-over-IP (VoIP). (Zhang & Liu, 2010) Σε ένα σύστημα υγειονομικής περίθαλψης, τόσο οι πληροφορίες υγειονομικής περίθαλψης που προσφέρονται από τους παρόχους όσο και οι ταυτότητες των χρηστών πρέπει να επαληθεύονται κατά την είσοδο.

Κρυπτογράφηση: Η κρυπτογράφηση δεδομένων είναι μια αποτελεσματική διαδικασία για την αποτροπή μη εξουσιοδοτημένης πρόσβασης ευαίσθητων δεδομένων. Η εφαρμογή της κρυπτογράφησης προστατεύει και διατηρεί την κυριότητα των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους - από το κέντρο δεδομένων έως το τελικό σημείο (συμπεριλαμβανομένων των κινητών συσκευών που χρησιμοποιούνται από γιατρούς, νοσηλευτές και διαχειριστές) και στο νέφος. Η κρυπτογράφηση είναι χρήσιμη για την αποφυγή έκθεσης σε παραβιάσεις, όπως παρακολούθηση πακέτων

(sniffing) και κλοπή συσκευών αποθήκευσης. Οι πάροχοι υπηρεσιών υγειονομικής περίθαλψης πρέπει να διασφαλίζουν ότι το σύστημα κρυπτογράφησης είναι αποτελεσματικό, εύχρηστο τόσο από τους ασθενείς όσο και από τους επαγγελματίες και είναι επεκτάσιμο για να μπορεί να συμπεριλάβει πιθανά νέα ηλεκτρονικά αρχεία υγείας. Αν και έχουν αναπτυχθεί διάφοροι αλγόριθμοι κρυπτογράφησης με καλές επιδόσεις (RSA, AES, RC6, DES, 3DES, IDEA, Blowfish κ.α. (Zhang & Liu, 2010)) η σωστή επιλογή των κατάλληλων αλγορίθμων κρυπτογράφησης για Big Data παραμένει ένα δύσκολο πρόβλημα.

Data Masking: Η κάλυψη δεδομένων είναι μια τεχνική που αντικαθιστά ευαίσθητα στοιχεία δεδομένων με μια μη αναγνωρίσιμη τιμή. Καθώς δεν αποτελεί τεχνική κρυπτογράφησης, η διαδικασία δεν είναι αντιστρέψιμη, οπότε δεν μπορεί να ανακτηθεί η αρχική τιμή που καλύφτηκε. Συνήθως περιλαμβάνονται ενέργειες όπως κάλυψη προσωπικών αναγνωριστικών όπως όνομα, αριθμός κοινωνικής ασφάλισης, στοιχεία γέννησης, ταχυδρομικός κώδικας κ.α.. Το data masking αποτελεί μια από τις δημοφιλείς λύσεις για ανωνυμοποίηση κρίσιμων δεδομένων. Παλαιότερες τεχνικές είναι η k-anonymity και η p-sensitivite anonymity που προστατεύουν τόσο την ταυτότητα του χρήστη όσο και το σχετικό θέμα. Άλλες μέθοδοι ανωνυμοποίησης χρησιμοποιούν προσθήκη θορύβου στα δεδομένα ή ανταλλαγή κελιών εντός στηλών στο σετ δεδομένων. Όλες οι παλιές αυτές μέθοδοι όμως δεν είναι αποτελεσματικές στο masking δεδομένων μεγάλης κλίμακας. (Archana et al., 2018)

Έλεγχος πρόσβασης: Μετά τον έλεγχο ταυτότητας οι χρήστες μπορούν να εισέλθουν σε ένα σύστημα πληροφοριών, αλλά η πρόσβασή τους εξακολουθεί να διέπεται από μια πολιτική ελέγχου πρόσβασης η οποία βασίζεται συνήθως στα προνόμια του προφίλ του χρήστη είτε είναι επαγγελματίας είτε ασθενής είτε κάποιος τρίτος. Η χορήγηση δικαιωμάτων είναι μια κρίσιμη διαδικασία η οποία πρέπει να γίνεται με προσοχή σε κάθε σύστημα πληροφοριών, ειδικά στον τομέα της υγείας. Συχνά παρέχονται εξελιγμένες δυνατότητες εξουσιοδότησης ώστε να διασφαλιστεί ότι οι χρήστες θα μπορούν να εκτελούν μόνο τις δραστηριότητες για τις οποίες έχουν δικαιώματα. Ο έλεγχος πρόσβασης βάσει ρόλου (RBAC) και ο έλεγχος πρόσβασης βάσει χαρακτηριστικών (ABAC) είναι τα πιο δημοφιλή μοντέλα για τον έλεγχο πρόσβασης στα

ηλεκτρονικά αρχεία υγείας EHR, αν και έχουν εμφανίσει περιορισμούς όταν χρησιμοποιούνται αποκλειστικά σε συστήματα υγείας (Fugkeaw et al., 2015). Για να ικανοποιηθούν οι απαιτήσεις για έλεγχο πρόσβασης υψηλής πολυπλοκότητας, όπως απαιτείται στην υγειονομική περίθαλψη, είναι απαραίτητη η υιοθέτηση τεχνολογιών που συνδυάζουν και τεχνικές ασφαλείας όπως η κρυπτογράφηση.

1.3.3 Τεχνολογίες Ιδιωτικότητας Big Data στην Υγεία

Τα τελευταία χρόνια έχει αυξηθεί η εμφάνιση εξελιγμένων επιθέσεων εναντίον πληροφοριακών συστημάτων, με κύριο σκοπό την παράνομη συλλογή δεδομένων από τον εισβολέα. Ο κίνδυνος της διαρροής προσωπικών δεδομένων είναι υπαρκτός και ειδικότερα στην υγεία υπάρχει μια αυξανόμενη ανησυχία λόγω της ιδιαίτερης ευαισθησίας των δεδομένων που είναι αποθηκευμένα ή που παράγονται από τα Big Data analytics. Η διαφορά με την ασφάλεια δεδομένων είναι ότι στη μεν ασφάλεια μας ενδιαφέρει η προστατευόμενη πρόσβαση καθ’ όλη τη διάρκεια του κύκλου ζωής των δεδομένων, ενώ η ιδιωτικότητα των δεδομένων ορίζει την πρόσβαση βάσει πολιτικών απορρήτου και νόμων που καθορίζουν, για παράδειγμα, ποιος μπορεί να δει προσωπικά δεδομένα, οικονομικές, ιατρικές ή άλλες εμπιστευτικές πληροφορίες. (Abouelmehdi et al., 2017). Η μη αποτελεσματική ιδιωτικότητα σε ευαίσθητα ιατρικά δεδομένα μπορεί να προκαλέσει περιστατικά όπως αυτό που περιγράφεται στο (Hill, 2012), όπου μια εταιρεία προώθησης διαφημιστικών κουπονιών (Target Corporation) απέστειλε κουπόνια για φροντίδα μωρού σε μια έφηβη κοπέλα η οποία δεν είχε ενημερώσει τους γονείς της για την εγκυμοσύνη. Αντίστοιχα περιστατικά όπως αυτό που αναφέρθηκε και στο περιοδικό Forbes επισημαίνουν τον κίνδυνο ότι η πρόσβαση σε Big Data πρέπει να διέπεται από ισχυρούς κανόνες ιδιωτικότητας ενώ οι προγραμματιστές του συστήματος θα πρέπει να επαληθεύουν ότι οι εφαρμογές τους συμμορφώνονται με τους κανόνες απορρήτου και ότι οι ευαίσθητες πληροφορίες παραμένουν ιδιωτικές ανεξάρτητα από τις αλλαγές στις εφαρμογές ή στους κανονισμούς απορρήτου.

Παρακάτω περιγράφονται μερικές από τις πιο δημοφιλείς μεθόδους διασφάλισης της ιδιωτικότητας στα Big Data. Παρόλο που αυτές οι τεχνικές χρησιμοποιούνται

παραδοσιακά για να διασφαλιστεί το απόρρητο του ασθενούς, τα μειονεκτήματά τους οδήγησαν στην έλευση νεότερων μεθόδων.

De-identification (απο-αναγνώριση): μια παραδοσιακή μέθοδος αποτροπής της διαρροής εμπιστευτικών πληροφοριών που κρύβει οποιεσδήποτε πληροφορίες που μπορούν να προσδιορίσουν τον ασθενή, είτε με αυτόματη διαδικασία αφαίρεσης συγκεκριμένων αναγνωριστικών του ασθενούς είτε με χειροκίνητη διαδικασία όπου ο ασθενής επιβεβαιώνει ότι τα δεδομένα δεν περιέχουν ευαίσθητες πληροφορίες. Εντούτοις, έρευνες έχουν δείξει ότι ένας εισβολέας μπορεί ενδεχομένως να λάβει ικανή εξωτερική πληροφόρηση, κάνοντας τη συγκεκριμένη τεχνική λιγότερο αποτελεσματική σε δεδομένα μεγάλης κλίμακας. Οι παραλλαγές k-ανωνυμίας, l-diversity και t-closeness έχουν προταθεί τα τελευταία χρόνια, κάνοντας την από-αναγνώριση πιο ελκυστική και αποτελεσματική σε εφαρμογές Big Data και κατ' επέκταση και στον τομέα της υγειονομικής περίθαλψης. (Li et al., 2007)

HybrEx: Το Hybrid Execution Model είναι ένα μοντέλο ιδιωτικότητας και απορρήτου στο cloud computing. Χρησιμοποιεί δημόσια «νέφη» μόνο για τα μη ευαίσθητα δεδομένα ενός οργανισμού που ταξινομεί ως δημόσια, δηλαδή όταν ο οργανισμός δηλώνει ότι δεν υπάρχει κίνδυνος απορρήτου κατά την εξαγωγή των δεδομένων και την εκτέλεση υπολογισμών σε αυτά. Αντίθετα η αποθήκευση και επεξεργασία δεδομένων που ο οργανισμός ταξινομεί ως ευαίσθητα γίνεται σε ιδιωτικό «νέφος». Επιπλέον, όταν μια εφαρμογή απαιτεί πρόσβαση τόσο στα ιδιωτικά όσο και στα δημόσια δεδομένα, η ίδια η εφαρμογή θα πρέπει να μπορεί να εκτελείται παράλληλα τόσο στα ιδιωτικά όσο και στα δημόσια νέφη. Για να λειτουργήσει το μοντέλο πρέπει να λαμβάνεται υπόψη η ευαισθησία των δεδομένων πριν από την εκτέλεση μιας εργασίας και να παρέχεται η κατάλληλη ασφάλεια με ανταλλαγή κλειδιών. (Ko et al., 2011)

Ανωνυμοποίηση βάσει ταυτότητας: Καθώς οι παραδοσιακές τεχνικές ανωνυμοποίησης δεν έχουν τα επιθυμητά αποτελέσματα στα Big Data, η Intel για να ανταποκριθεί στις προκλήσεις του Cloud Computing δημιούργησε μια ανοιχτή αρχιτεκτονική για ανωνυμοποίηση που επέτρεψε να χρησιμοποιηθούν διάφορα εργαλεία τόσο για την απο-αναγνώριση όσο και για την επαν-αναγνώριση αρχείων ιστού. Η Intel

διαπίστωσε ότι παρά την κάλυψη (masking) συνηθισμένων πληροφοριών ταυτοποίησης όπως ονόματα χρήστη και IP διευθύνσεις, τα ανώνυμα δεδομένα παρέμεναν ανυπεράσπιστα έναντι επιθέσεων συσχέτισης και προχώρησε σε περαιτέρω ανωνυμοποίηση δεδομένων τα οποία συσχέτιζαν τους μεμονωμένους χρήστες με φαινομενικά άσχετα δεδομένα. Η δράση της Intel αποτελεί μια μελέτη περίπτωσης της εφαρμογής ανωνυμοποίησης σε μια επιχείρηση, που περιγράφει τις απαιτήσεις, την εφαρμογή και τις εμπειρίες που συναντήθηκαν κατά τη χρήση της ανωνυμοποίησης για την προστασία της ιδιωτικότητας, σε εταιρικά δεδομένα που αναλύθηκαν χρησιμοποιώντας τεχνικές Big Data. Το συμπέρασμα είναι ότι η ανωνυμοποίηση πρέπει να είναι κάτι περισσότερο από απλή κάλυψη ορισμένων πεδίων και τα ανωνυμοποιημένα σύνολα δεδομένων πρέπει να αναλυθούν προσεκτικά για να προσδιοριστεί εάν είναι ευάλωτα σε επίθεση. (Sedayao et al., 2014)

1.3.4 Big Data στην Υγεία και Ethics

Δύο δεκαετίες μετά την ολοκλήρωση του Προγράμματος Ανθρώπινου Γονιδιώματος (Human Genoce Project), έχουν δοθεί πλήθος νομοθετικών και πολιτικών απαντήσεων στα ερωτήματα σχετικά με τους κοινωνικοοικονομικούς κινδύνους ασφάλειας που δημιουργήθηκαν από την αύξηση της έρευνας γενετικών δεδομένων, των βιολογικών τραπεζών και των σχετικών βάσεων δεδομένων. Σχετικά με τα ζητήματα ιδιωτικότητας που απορρέουν από τη χρήση αυτών των δεδομένων καθώς και πιθανές γενετικές διακρίσεις, είναι αξιοσημείωτο ότι ακόμη και μια χώρα με αξιοσημείωτη υγειονομική περίθαλψη όπως ο Καναδάς, μόλις το 2017 υιοθέτησε τη νομοθεσία που απαγορεύει τη χρήση γενετικών δεδομένων από ασφαλιστές ζωής, ακολουθώντας το παράδειγμα των ευρωπαϊκών χωρών (Joly et al., 2017). Απαντώντας στις σύγχρονες προκλήσεις, το Συμβούλιο της Ευρώπης συνέστησε το 2016 να μη χρησιμοποιούνται γενετικές δοκιμές για ασφαλιστικούς σκοπούς (Knoppers & Thorogood, 2017). Τέλος, οι Ηνωμένες Πολιτείες ενέκριναν το νόμο περί μη διάκρισης γενετικών δεδομένων (Genetic Information Nondiscrimination Act - GINA) όσον αφορά την ασφάλιση υγείας και την απασχόληση το 2008.

Ένα άλλο σημείο ανησυχίας περιστρέφεται γύρω από τους κανόνες συγκατάθεσης για τη χρήση δεδομένων υγείας, συμπεριλαμβανομένων των γενετικών δεδομένων. Η δημιουργία εθνικών βιολογικών πόρων με τη μορφή μεγάλων βάσεων δεδομένων για μελλοντική έρευνα απροσδιόριστης μορφής εγείρει σημαντικά ερωτήματα με το είδος της συγκατάθεσης που έχει ζητηθεί από τους συμμετέχοντες, τη νομιμότητα μιας τέτοιας συγκατάθεσης και τους κανόνες δεοντολογίας που θα πρέπει να διέπει η σχετική έρευνα όποτε αυτή πραγματοποιηθεί. Σήμερα, η συγκατάθεση ευρέως σκοπού αναγνωρίζεται στο Συμβούλιο Διεθνών Οργανισμών Ιατρικών Επιστημών (CIOMS) (CIOMS, 2016). Οι φόβοι για κατάχρηση αυτού του είδους των συναινέσεων έχουν μετριαστεί σε κάποιο βαθμό από τη νομοθεσία των περισσότερων χωρών για τις γενετικές διακρίσεις και από την ανάπτυξη εξελιγμένων μηχανισμών ασφάλειας, αλλά παραμένουν ως γενικότερες ανησυχίες για την προστασία της ιδιωτικής ζωής. Τέλος, η τεχνική της αλληλουχίας γονιδιώματος με χρήση Big Data είναι πιθανό να αποκαλύψει απρόβλεπτες πληροφορίες καθώς συνεχώς βελτιώνεται η δυνατότητα των ερευνητών να ερμηνεύσουν τα αποτελέσματα, το οποίο μπορεί να προκαλέσει απρόβλεπτες καταχρήσεις τρίτων πάνω σε αυτές τις μελλοντικές νέες ερμηνείες (Wagner et al., 2014).

Το «δικαίωμα στην επιστήμη»

Οι συγγραφείς (Knoppers & Thorogood, 2017) αναφέρονται στη συζήτηση για τους κινδύνους από την κακή χρήση των Big Data (ειδικότερα στην υγεία) και πρεσβεύουν ότι το βάρος της συζήτησης θα έπρεπε να πέφτει κυρίως στο δικαίωμα όλων «να συμμετάσχουν στην επιστημονική πρόοδο και τα οφέλη της». Αυτό το δικαίωμα αναφέρουν ότι έχει τις ρίζες του στην Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων του 1948 (Assembly UN, 1948) και έγινε νομικά δεσμευτικό βάσει του Διεθνούς Συμφώνου για τα Οικονομικά, Κοινωνικά και Πολιτιστικά Δικαιώματα του 1966, το οποίο υπογράφηκε και επικυρώθηκε από 165 χώρες (Assembly UN, 1966). Λόγω του status ως ανθρώπινο δικαίωμα που θεσμοθετήθηκε από το διεθνές δίκαιο, το «δικαίωμα στην επιστήμη» έχει καθολική ισχύ και ξεπερνάει τα στεγανά της «βιοηθικής», επιβάλλοντας από τα κράτη να αναλάβουν θετικά σχετικά καθήκοντα (Knoppers et al., 2011). Μέχρι τώρα, υπήρξαν περιορισμένες προσπάθειες για την εφαρμογή αυτού του δικαιώματος στην επιστήμη από λίγες χώρες.

Το 2014, η Παγκόσμια Συμμαχία για τη Γονιδιωματική και την Υγεία (GA4GH) άρχισε να εξετάζει μια πιθανή πτυχή του δικαιώματος στην επιστήμη. Έτσι, δημιουργήθηκε ένα πλαίσιο κοινοποίησης γονιδιωματικών και υγειονομικών δεδομένων μαζί με τις συνδεόμενες πολιτικές σχετικές με τη συναίνεση, το απόρρητο και την ασφάλεια τα οποία επικεντρώνονται στην περαιτέρω επεξεργασία αυτού του δικαιώματος στο πλαίσιο της επιστημών που απαιτούν Big Data. Εστιάζοντας στην εντατική έρευνα δεδομένων, η GA4GH επιδιώκει να διευκολύνει την παγκόσμια κοινή χρήση δεδομένων μέσω της δημιουργίας πολιτικών ενεργοποίησης, πληροφορικής και εργαλείων. Για να γίνει αυτό, οι πολιτικές και τα εργαλεία που δημιουργούνται από τα μέλη οφείλουν να αντιμετωπίζουν δύσκολα ζητήματα όπως η κοινή χρήση δεδομένων παλαιού τύπου (legacy data) και η σύγκριση κινδύνων σε σχέση με τα οφέλη που προκύπτουν από την παραδοσιακή παρεμβατική ιατρική και από την αναλυτική δεδομένων μεγάλης κλίμακας. (Knoppers, 2014)

Αξίζει να εξεταστεί αν η μέχρι τώρα αντιπαράθεση μεταξύ των ζητημάτων ιδιωτικότητας και ασφάλειας και τα οφέλη της κοινής χρήσης δεδομένων μεγάλης κλίμακας παραμένει. Την τελευταία δεκαετία ήμασταν μάρτυρες τόσο της αναγνώρισης της ανάγκης επιτάχυνσης της εναρμόνισης των ρυθμιστικών πλαισίων στην Ευρώπη για έρευνα και ανταλλαγή δεδομένων σχετικών με την υγεία όσο και για την αποδοχή ευρείας συναίνεσης για μελλοντικές μη καθορισμένες χρήσεις και τη διεθνή ανταλλαγή δεδομένων υπό την προϋπόθεση ότι υπάρχει επαρκής έλεγχος και διαχείριση. Ομοίως, οι συστάσεις του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης το 2017 (OECD) σχετικά με τη διαχείριση δεδομένων υγείας προβλέπουν μέτρα για τη διασφάλιση περισσότερης (όχι λιγότερης) ανταλλαγής δεδομένων, ώστε να μεγιστοποιηθούν τα πιθανά οφέλη για την υγεία και να «διαχειριστούμε τους κινδύνους διατηρώντας παράλληλα τη χρησιμότητα δεδομένων προσωπικής υγείας για το δημόσιο συμφέρον σε αποτελεσματικά και βιώσιμα συστήματα υγειονομικής περίθαλψης» (OECD, 2015).

1.3.5 GDPR

Ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR), ο οποίος εφαρμόστηκε σε όλα τα κράτη μέλη της ΕΕ από τις 25 Μαΐου 2018,

αποτελεί ορόσημο στην εξέλιξη του ευρωπαϊκού πλαισίου προστασίας της ιδιωτικότητας (European Law, 2016). Ο κανονισμός αυτός έχει ευρύ παγκόσμιο αντίκτυπο, καθοδηγούμενος από μια φιλοσοφική προσέγγιση στην προστασία των δεδομένων, βασισμένη στην έννοια της ιδιωτικής ζωής ως θεμελιώδους ανθρώπινου δικαιώματος (όπως κατοχυρώνεται στον Χάρτη των Δικαιωμάτων της ΕΕ). Ο νέος νόμος καλύπτει τα προσωπικά δεδομένα όλων των κατοίκων της ΕΕ, ανεξάρτητα από την τοποθεσία που γίνεται η επεξεργασία. Τα προσωπικά δεδομένα είναι πληροφορίες που, άμεσα ή έμμεσα, μπορούν να προσδιορίσουν ένα άτομο και συγκεκριμένα περιλαμβάνουν διαδικτυακά αναγνωριστικά όπως διευθύνσεις IP, cookies και ψηφιακά δακτυλικά αποτυπώματα και δεδομένα τοποθεσίας που θα μπορούσαν να προσδιορίσουν ένα άτομο. Αυτός ο ορισμός είναι πολύ ευρύτερος από την έννοια των προσωπικά αναγνωρίσιμων πληροφοριών σύμφωνα με τη νομοθεσία περί απορρήτου των ΗΠΑ. (Goddard, 2017)

Το GDPR διέπεται από αρχές (περιορισμός σκοπού, ελαχιστοποίηση δεδομένων, ακρίβεια,ακεραιότητα), αλλά η προστασία δεδομένων βρίσκεται στον πυρήνα της ουσίας του GDPR. Στοχεύει τόσο στη διαφάνεια (διασφαλίζοντας ότι παρέχονται πλήρεις πληροφορίες σε άτομα με προσιτό τρόπο) όσο και στην υπευθυνότητα (διασφαλίζοντας ότι όλοι οι οργανισμοί αναλαμβάνουν αποδεδειγμένη ευθύνη όταν χρησιμοποιούν προσωπικά δεδομένα). Η λειτουργία και η ενσωμάτωση αυτών των αρχών στον ερευνητικό κύκλο απαιτεί τον προληπτικό σχεδιασμό της ιδιωτικότητας ως βασική προϋπόθεση για οποιαδήποτε εργασία συλλογής δεδομένων. Πρέπει επίσης να ενσωματωθεί τόσο στα συστήματα σχεδιασμού οποιασδήποτε αρχιτεκτονικής IoT όσο και στις γενικές οργανωτικές πρακτικές ερευνητικών οργανισμών. (Voigt et al., 2017)

Μια βασική αλλαγή που πρέπει να σημειωθεί σε σχέση με το παρελθόν είναι η ξεκάθαρη απαίτηση για συναίνεση. Η συγκατάθεση στο πλαίσιο του GDPR πρέπει να παρέχεται ελεύθερα, να είναι συγκεκριμένη, να ενημερώνεται συχνά και να αποδεικνύεται με σαφή θετική ενέργεια από τον χρήστη. Πρέπει επίσης να είναι επαληθεύσιμη και όταν τα δεδομένα είναι ευαίσθητα, να ζητείται υψηλότερο επίπεδο ρητής συγκατάθεσης. Η επεξεργασία δεδομένων είναι επιτρεπτή μόνο εάν είναι διαφανής και αυτό σημαίνει ότι πρέπει να υπάρχει διαφάνεια στην επεξεργασία δεδομένων μέσω αποτελεσματικής επικοινωνίας με τους ενδιαφερόμενους. Σύμφωνα με το πλαίσιο του

GDPR εκτεταμένες πληροφορίες πρέπει να παρέχονται στους χρήστες, συμπεριλαμβανομένων λεπτομερειών σχετικά με τους παραλήπτες, τις περιόδους διατήρησης και το εύρος των ατομικών τους δικαιωμάτων, όπως η πρόσβαση και η φορητότητα. Όλα αυτά πρέπει να παρέχονται σε προσιτή γλώσσα για να διασφαλιστεί ότι μπορεί να γίνουν εύκολα κατανοητά. (Goddard, 2017)

Εκτός από τα κανονικά προσωπικά δεδομένα, το GDPR καθορίζει ότι ορισμένα δεδομένα είναι πιο ευαίσθητα. Τα δεδομένα που αφορούν την υγεία ανήκουν σε αυτή την ειδική κατηγορία. Ορισμένα από τα δεδομένα που δημιουργούνται με τη χρήση εφαρμογών ενδέχεται να θεωρούνται δεδομένα που αφορούν την υγεία, απολαμβάνοντας έτσι αυστηρότερους κανόνες απορρήτου, δεδομένης της πιθανής επίδρασης στη ζωή του χρήστη, εάν αυτά τα δεδομένα είναι ελεύθερα διαθέσιμα. Το GDPR, κατ' αρχήν, απαγορεύει την επεξεργασία αυτών των ειδών δεδομένων, εκτός εάν πληρείται μία από τις εξαιρέσεις του Άρθρου 9. Η πρώτη εξαίρεση είναι οι ιδιοκτήτες των δεδομένων να έχουν δώσει τη ρητή συγκατάθεσή τους για την επεξεργασία και η δεύτερη εξαίρεση αναφέρεται σε προσωπικά δεδομένα που χρησιμοποιούνται για ιατρική διάγνωση ή την παροχή υγειονομικής περίθαλψης. Επιπρόσθετα το άρθρο αναφέρει ότι ισχύει μόνο όταν τα δεδομένα υποβάλλονται σε επεξεργασία «από ή υπό την ευθύνη ενός επαγγελματία που υπόκειται στην υποχρέωση επαγγελματικού απορρήτου». (Mulder, 2019)

Όταν εμπορικές εφαρμογές και οι αντίστοιχες φορετές συσκευές (wearbales) χρησιμοποιούνται σε ιατρικό πλαίσιο, πρέπει να εξεταστεί αν πληρείται αυτή η απαίτηση (ότι η επεξεργασία γίνεται από άτομο που υπόκειται στην υποχρέωση επαγγελματικού απορρήτου), λαμβάνοντας υπόψη ότι τα δεδομένα αποθηκεύονται στη συσκευή τους ή στους διακομιστές του παρόχου της εφαρμογής. Επιπλέον, καθώς η εφαρμογή καθορίζει ακριβώς ποια δεδομένα συλλέγονται, πιθανώς υπάρχουν περισσότερα δεδομένα που υποβάλλονται σε επεξεργασία από τα απαραίτητα για τη θεραπεία του ασθενούς. Τέλος, υπάρχουν εφαρμογές που έχουν αναπτυχθεί ειδικά για τον τομέα της υγείας. Σύμφωνα με το Οδηγία 2007/47/ ΕC, αυτές οι εφαρμογές θεωρούνται ιατρο-τεχνολογικά προϊόντα. Για αυτές τις εφαρμογές, τα δεδομένα πρόκειται να υποβληθούν σε επεξεργασία υπό την ευθύνη του ιατρού και επομένως δεν απαιτείται συγκατάθεση. (Mulder, 2019)

2 Μελέτες Περίπτωσης

2.1 Εισαγωγή

Οι οργανισμοί υγειονομικής περίθαλψης είναι κρίσιμο να διαχειρίζονται και να διαφυλάσσουν τα προσωπικά στοιχεία που αποθηκεύουν και να αντιμετωπίζουν τους κινδύνους και τις νομικές τους ευθύνες σε σχέση με την επεξεργασία προσωπικών δεδομένων, ώστε να αντιμετωπίσουν τον αυξανόμενο όγκο της ισχύουσας νομοθεσίας περί προστασίας δεδομένων. Οι χώρες έχουν διαφορετικές πολιτικές και νόμους για το απόρρητο των δεδομένων. Στον παρακάτω πίνακα αναφέρονται οι κανονισμοί και οι νόμοι για την προστασία των δεδομένων σε ορισμένες από αυτές.

Χώρα	Νομοθεσία	Χαρακτηριστικά
ΗΠΑ	HIPAA Act Patient Safety and Quality Improvement Act (PSQIA) HITECH Act	Απαιτεί τη θέσπιση εθνικών προτύπων για ηλεκτρονικές συναλλαγές υγειονομικής περίθαλψης. Δίνει το δικαίωμα στην ιδιωτική ζωή σε άτομα ηλικίας 12 έως 18 ετών. Απαιτείται υπογεγραμμένη άδεια από τον ασθενή πριν δοθούν οποιεσδήποτε πληροφορίες σχετικά με την παρεχόμενη υγειονομική περίθαλψη σε οποιονδήποτε, συμπεριλαμβανομένων των γονέων. Το άτομο που παραβιάζει τις διατάξεις περί ιδιωτικότητας υπόκειται σε αστικές ποινές. (DLA, 2017)
Ε.Ε.	Οδηγία για προστασία δεδομένων	Προστατεύει τα θεμελιώδη δικαιώματα και τις ελευθερίες των ανθρώπων και ιδίως το δικαίωμά τους στην ιδιωτική ζωή σε σχέση με την επεξεργασία προσωπικών δεδομένων. (Craig & Ludloff, 2011)
Καναδάς	Personal Information Protection and Electronic Documents Act (‘PIPEDA')	Κάθε άτομο έχει το δικαίωμα να γνωρίζει τους λόγους συλλογής ή χρήσης προσωπικών πληροφοριών, ενώ οι οργανισμοί υποχρεούνται να προστατεύουν αυτές τις πληροφορίες με ασφαλή τρόπο. (Jensen, 2013)
Ην.	Data Protection	Παρέχει τη δυνατότητα στα άτομα να ελέγχουν τις

Βασίλειο	Act (DPA)	πληροφορίες για τον εαυτό τους. Τα προσωπικά δεδομένα δεν μπορούν να διαβιβάζονται σε χώρες εκτός της Ε.Ε., εκτός αν η χώρα διασφαλίζει επαρκές επίπεδο προστασίας για τα δικαιώματα και τις ελευθερίες των πολιτών σε σχέση με τα προσωπικά δεδομένα. (Butler, 2018)
Μαρόκο	Νόμος 09-08	Προστατεύει την ιδιωτικότητα ενός ατόμου περιορίζοντας τη χρήση προσωπικών και ευαίσθητων δεδομένων από τρίτους. (Makulilo, 2016)
Ρωσία	Ρωσικός ομοσπονδιακός νόμος για τα προσωπικά δεδομένα	Απαιτεί από τους χειριστές δεδομένων να λάβουν «όλα τα απαραίτητα οργανωτικά και τεχνικά μέτρα που απαιτούνται για την προστασία των προσωπικών δεδομένων από παράνομη ή τυχαία πρόσβαση».(Carrie & Bykovksy, 2016)
Ινδία	IT Act and IT (Amendment) Act	Απαιτεί την εφαρμογή πρακτικών ασφαλείας για ευαίσθητα προσωπικά δεδομένα. Προβλέπει αποζημίωση σε άτομο που επηρεάζεται από διαρροή δεδομένων. Προβλέπει φυλάκιση ή πρόστιμο για ένα άτομο που προκαλεί αδικαιολόγητη διαρροή αποκαλύπτοντας προσωπικά στοιχεία άλλου ατόμου, ενώ παρέχει υπηρεσίες σύμφωνα με τους νόμιμους όρους. (Greenleaf, 2011)
Βραζιλία	Σύνταγμα	Η ιδιωτικότητα του λαού είναι απαραβίαστη, με εγγυημένο δικαίωμα αποζημίωσης από υλικές ή ηθικές βλάβες που προκύπτουν από την παραβίαση της. (Doneda & Mendes, 2014)
Αγκόλα	Νόμος προστασίας δεδομένων	Η συλλογή και η επεξεργασία ευαίσθητων δεδομένων επιτρέπονται μόνο όταν υπάρχει νομική διάταξη που επιτρέπει την εν λόγω επεξεργασία. (Traca & Embry, 2012)

Στις επόμενες υποενότητες αναλύεται η νομοθεσία για δεδομένα μεγάλης κλίμακας γενικότερα και ειδικότερα στον τομέα της υγείας για τις εξής χώρες: Ελλάδα, Γερμανία, ΗΠΑ, Καναδάς και Ιαπωνία. Οι λόγοι που επιλέχθηκαν αυτές οι χώρες (εκτός από την Ελλάδα που επιλέχθηκε για προφανείς λόγους) είναι ότι αποτελούν είτε ισχυρές οικονομίες στην περιοχή τους (ΗΠΑ, Γερμανία, Ιαπωνία), είτε έχουν επιδείξει σημαντική ωριμότητα σε θέματα αντιμετώπισης της δημόσιας υγείας (Καναδάς). Επιπρόσθετα

αποτελούν χώρες με υψηλή τεχνολογική εξέλιξη, όπου και τα Big Data θα έχουν σημαντική παρουσία σε όλες τις δραστηριότητες της υγείας.

2.2 Ελλάδα

2.2.1 Νομοθεσία

Το δικαίωμα της ιδιωτικότητας στους Έλληνες πολίτες κατοχυρώνεται από το Σύνταγμα (άρθρο 9), ενώ επιπρόσθετα κατοχυρώνεται και το δικαίωμα προστασίας των προσωπικών δεδομένων. Συγκεκριμένα το Άρθρο 9^{A} αναφέρει ότι «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει» (Βουλη, 2020). Με βάση αυτή την αρχή της ιδιωτικότητας των δεδομένων που απορρέει από το Σύνταγμα, πλήθος άλλων νόμων καλείται να παρέχει τις λεπτομέρειες εφαρμογής αυτού του συνταγματικού δικαιώματος. Η ασφαλής επεξεργασία των προσωπικών δεδομένων ρυθμίζεται με τους παρακάτω νόμους: ν. 2472/1997, ν.3471/2006 και ν.4624/2019.

Νόμος 2472/1997 (Προϊσχύον νομοθέτημα). Ο Νόμος 2472/1997 αποτελεί εφαρμογή της Οδηγίας 95/46/ΕΚ (της Ευρωπαϊκής Ένωσης με βασικό στόχο «τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής» (άρθρο 1). Ο νόμος επίσης θεσπίζει τη δημιουργία μιας ανεξάρτητης διοικητικής Αρχής, η Αρχή Προστασίας Προσωπικών Δεδομένων, «με αποστολή την εποπτεία της εφαρμογής του παρόντος νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά». (DPA, 2020)

Η επεξεργασία προσωπικών δεδομένων διεξάγεται αποκλειστικά από άτομα τα οποία ελέγχονται από τον υπεύθυνο επεξεργασίας και μόνο κατ' εντολή του (άρθρο 10). Τα άτομα που επεξεργάζονται προσωπικά δεδομένα (υπεύθυνοι επεξεργασίας) οφείλουν

να λαμβάνουν τα κατάλληλα μέτρα διασφάλισης του επιπέδου ασφαλείας που είναι ανάλογο με την ευαισθησία των δεδομένων που επεξεργάζονται και τους κινδύνους που συνεπάγεται η ενέργεια τους. Για την εκτίμηση του κινδύνου που ενδέχεται να υπάρξει με την επεξεργασία των δεδομένων απαιτείται η ανάλυση επικινδυνότητας (risk analysis), η οποία έχει στόχο την εκτίμηση των απειλών και επιθέσεων από κακόβουλους, στις οποίες είναι εκτεθειμένο το πληροφοριακό σύστημα στο οποίο είναι αποθηκευμένα τα δεδομένα και όπου πραγματοποιείται η επεξεργασία. Με βάση αυτή την ανάλυση, ο υπεύθυνος επεξεργασίας οφείλει να δράσει κατάλληλα για να μειώσει τον κίνδυνο σε αποδεκτά όρια. (DPA, 2020)

Ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με σαφή τρόπο το άτομο στο οποίο ανήκουν τα δεδομένα για τα παρακάτω στοιχεία τουλάχιστον: την ταυτότητά του, τον σκοπό της επεξεργασίας, τους αποδέκτες των δεδομένων, την ύπαρξη του δικαιώματος πρόσβασης. Επιπλέον, οι υπεύθυνοι επεξεργασίας, οφείλουν να επιλέγουν τα κατάλληλα πρόσωπα με αντίστοιχα επαγγελματικά προσόντα ώστε να μπορούν να παρέχουν επαρκείς εγγυήσεις σε σχέση με τις γνώσεις και την ακεραιότητά τους για την τήρηση της ιδιωτικότητας αλλά και να παίρνουν τα απαραίτητα οργανωτικά και τεχνικά μέτρα για την ασφάλεια και την προστασία των προσωπικών δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, διάδοση ή κάθε άλλη μορφή αθέμιτης επεξεργασίας.

Ο Νόμος επιτρέπει τη συλλογή και την επεξεργασία ευαίσθητων προσωπικών δεδομένων υγείας, αλλά και τη δημιουργία του σχετικού αρχείου, μετά από αδειοδότηση από την Αρχή Προστασίας Προσωπικών Δεδομένων Αρχής, υπό την προϋπόθεση το άτομο που εκτελεί την επεξεργασία αποτελεί επαγγελματία υγείας και υπόκειται στο καθήκον της εχεμύθειας, υποχρεωμένος σε συναφή κώδικα δεοντολογίας. Επίσης απαραίτητη προϋπόθεση είναι η επεξεργασία δεδομένων υγείας να είναι χρήσιμη για την ιατρική πρόληψη και περίθαλψη ή τη διαχείριση γενικότερων υπηρεσιών υγείας, ερευνητικών ή επιστημονικών σκοπών και γενικά για βελτίωση της υγείας στην Ελλάδα. Τέλος απαραίτητη είναι και η υποχρέωση της ανωνυμοποίησης των δεδομένων που λαμβάνονται για τη διασφάλιση της ιδιωτικότητας των προσώπων στα οποία αναφέρονται τα δεδομένα (άρθρο 7). (DPA, 2020)

Νόμος 3471/2006. Σκοπός του νόμου είναι «η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών». Αποτελεί ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Στο άρθρο 4 ο Νόμος αναφέρει ότι οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, προστατεύεται από το απόρρητο των επικοινωνιών. Σε σχέση με την επεξεργασία προσωπικών δεδομένων αναφέρει στο άρθρο 5 ότι είναι επιτρεπτή μόνο αν (α) ο χρήστης μετά από ενημέρωση για το είδος των δεδομένων, το σκοπό και την έκταση της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών έχει συγκατατεθεί, ή (β) η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία ο χρήστης είναι συμβαλλόμενο μέρος. Επιπρόσθετα για τα δεδομένα κίνησης, ο φορέας παροχής των υπηρεσιών οφείλει να ενημερώσει τον συνδρομητή ή τον χρήστη πριν από τη χορήγηση της συγκατάθεσής του σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία και τη διάρκεια της επεξεργασίας αυτής.

Ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα, προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του καθώς και η ασφάλεια του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών. Τα μέτρα αυτά, εφόσον είναι αναγκαίο, πρέπει να λαμβάνονται από κοινού με τον πάροχο του δημοσίου δικτύου και να εγγυώνται επίπεδο ασφάλειας ανάλογο προς τον υπάρχοντα κίνδυνο, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες καθώς και του κόστους εφαρμογής τους (άρθρο 12). Κατά την εφαρμογή των ανωτέρω στα πληροφοριακά συστήματα υγείας όπου χρησιμοποιείται το δημόσιο δίκτυο επικοινωνιών, οι πάροχοι του δικτύου και του

πληροφοριακού συστήματος ή της πλατφόρμας οφείλουν να συνεργάζονται αρμονικά και να ληφθούν όλες οι απαραίτητες ενέργειες που θα διαφυλάξουν το απόρρητο της επικοινωνίας και ανταλλαγής δεδομένων.

Επιπρόσθετα υπάρχει ο **νόμος 3418/2005** (Κώδικας Ιατρικής Δεοντολογίας) που αναφέρει ότι ο ιατρός λαμβάνει όλα τα αναγκαία μέτρα, έτσι ώστε στην περίπτωση επιστημονικών δημοσιεύσεων να μην γνωστοποιείται με οποιονδήποτε τρόπο η ταυτότητα του ασθενή στον οποίο αφορούν τα δεδομένα. Εάν, λόγω της φύσης της δημοσίευσης, είναι αναγκαία η αποκάλυψη της ταυτότητας του ασθενή ή στοιχείων που υποδεικνύουν ή μπορούν να οδηγήσουν στην εξακρίβωση της ταυτότητάς του, απαιτείται η ειδική έγγραφη συναίνεσή του. Επίσης ο ιατρός τηρεί τα επαγγελματικά του βιβλία με τέτοιο τρόπο, ώστε να εξασφαλίζεται το ιατρικό απόρρητο και η προστασία των προσωπικών δεδομένων. Ο ασθενής έχει δικαίωμα πρόσβασης στα ιατρικά αρχεία, καθώς και λήψης αντιγράφων του φακέλου του. Δεν επιτρέπεται σε τρίτο η πρόσβαση στα ιατρικά αρχεία ασθενή. Κατ' εξαίρεση επιτρέπεται η πρόσβαση στις δικαστικές και εισαγγελικές αρχές κατά την άσκηση των καθηκόντων τους. Τέλος, ο ασθενής έχει το δικαίωμα πρόσβασης, σύμφωνα με τις οικείες διατάξεις, στα εθνικά ή διεθνή αρχεία στα οποία έχουν εισέλθει τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν. (Lawspot, 2005)

GDPR. Από την 25^{η} Μαΐου 2018, η βασική νομοθεσία για την προστασία των δεδομένων στην Ευρωπαϊκή Ένωση(βλ.Κεφάλαιο Γερμανία).

Νόμος 4624/2019. Σκοπός του νόμου είναι η λήψη μέτρων εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και η ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού

χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. **Επί της ουσίας ο νόμος εκτελεί την οδηγία General Data Protection Regulation – GDPR που αναφέρθηκε σε προηγούμενη ενότητα.** (DPA, 2020)

Ο Νόμος καθορίζει ρητά το πλαίσιο με το οποίο προστατεύονται τα προσωπικά δεδομένα από την επεξεργασία. Καθώς υπάρχουν αρκετά ασαφή σημεία, η Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα οφείλει να γνωμοδοτεί κατά περίπτωση, αξιολογώντας τις ειδικές περιστάσεις που υπάρχουν. Η σημασία που δίνει ο νόμος στην Αρχή είναι εμφανής από την εκτενή αναφορά στη ρύθμιση της λειτουργίας της. Σχετικά με την υγεία, ιδιαίτερη αναφορά γίνεται στην προστασία των γενετικών δεδομένων, η επεξεργασία των οποίων απαγορεύεται ρητά είτε για σκοπούς ασφάλισης είτε για άλλους σκοπούς. Η συγκεκριμένη διάταξη καλύπτει ένα νομικό κενό το οποίο υπήρχε στην ελληνική νομοθεσία καθώς ενώ παλαιότερα η διενέργεια εξετάσεων για τον έλεγχο της ασφαλιστικής ικανότητας φυσικού προσώπου ήταν μεμπτή, πλέον έχει καταστεί παράνομη εκ του νόμου. (DPA, 2020)

Ενδιαφέρον σημείο είναι και το Άρθρο 23 του Νόμου, όπου και προβλέπεται η απαίτηση συγκατάθεσης για επεξεργασία προσωπικών δεδομένων σε περίπτωση ανήλικου υποκείμενου. Συγκεκριμένα, προβλέπει ότι η συγκατάθεση επιτρέπεται μόνο εφόσον ο ανήλικος έχει συμπληρώσει το 15^{ο} έτος ηλικίας, ενώ κάτω από αυτό το όριο δεν επιτρέπεται καμία επεξεργασία. Αυτός ο περιορισμός είναι λιγότερο αυστηρός από τον ευρωπαϊκό νόμο GDPR ο οποίος θέτει ως όριο τα 16, αλλά επιτρέπει τις εθνικές νομοθεσίες να κατεβάσουν το όριο αυτό στα 13 έτη. Το αποτέλεσμα αυτού του άρθρου είναι ότι καθίστανται άκυρες οι συγκαταθέσεις για άτομα κάτω των 15 ετών. Αυτό δημιουργεί κάποια προβλήματα εφαρμογής καθώς είναι συχνά δύσκολη η αποτελεσματική ταυτοποίηση ηλεκτρονικής συγκατάθεσης, ενώ δημιουργεί περαιτέρω προβλήματα σε δεδομένα μεγάλης κλίμακας, όπου η συγκατάθεση γενικά είναι προβληματική, ιδιαίτερα αν εμπλέκονται και άτομα κάτω των 15 ετών.

2.2.2 Ιδιωτικότητα και Υγεία

Τα ευαίσθητα προσωπικά δεδομένα που αφορούν στην υγεία συλλέγονται από γιατρούς και νοσηλευτικά ιδρύματα με συνηθέστερο σκοπό την παροχή ιατρικής φροντίδας και άλλων υπηρεσιών υγείας. Κάθε άλλη επεξεργασία που γίνεται πέραν του προαναφερόμενου σκοπού της παροχής ιατρικής φροντίδας ή υπηρεσιών υγείας πρέπει να γνωστοποιείται στην Αρχή και να λαμβάνεται σχετική άδεια από αυτήν. (Παναγοπουλου & Κουτνατζη, 2015)

Το υποκείμενο πρόσωπο στο οποίο αφορούν τα δεδομένα υγείας διατηρεί το δικαίωμα πρόσβασης σε προσωπικά ή μη δεδομένα υγείας που συλλέγονται και υπόκεινται σε επεξεργασία. Το δικαίωμα αυτό ορίζει ότι ο ασθενής έχει δικαίωμα πρόσβασης στα ιατρικά αρχεία, αλλά και στη λήψη αντιγράφων του φακέλου του, ενώ αυτό δεν μπορεί να απορριφθεί από τον ιατρό για λόγους ιατρικού απόρρητου. Το υποκείμενο πρόσωπο μπορεί να αιτηθεί την πρόσβαση στα ιατρικά αρχεία του στον υπεύθυνο επεξεργασίας (ιατρός ή υπεύθυνος νοσηλευτικού ιδρύματος) είτε άμεσα είτε μέσω εξουσιοδοτημένου εκπροσώπου. Ένας τρίτος μπορεί να αιτηθεί τη χορήγηση προσωπικών δεδομένων σε ένα ίδρυμα, αιτιολογώντας το λόγο και τους σκοπούς αυτής της συλλογής δεδομένων προς την Αρχή, η οποία θα εξετάσει και θα απαντήσει σχετικά θετικά ή αρνητικά. (Παναγοπουλου & Κουτνατζη, 2015)

Στην εποχή των Big Data, και στην Ελλάδα υπάρχει η ανάγκη για συλλογή δεδομένων για λόγους έρευνας. Σύμφωνα με την κείμενη νομοθεσία, επιτρέπεται μετά από έγκριση της Αρχής, η οποία κρίνει παγίως ότι η διενέργεια επιστημονικής έρευνας συνιστά νόμιμο σκοπό επεξεργασίας, μεταξύ άλλων, και λόγω του ότι σύμφωνα με το άρθρο 16 του Συντάγματος η ανάπτυξη και η προαγωγή της έρευνας αποτελεί υποχρέωση του Κράτους. Επομένως η Αρχή κατά κύριο λόγο γνωμοδοτεί υπέρ της χρήσης προσωπικών δεδομένων υγείας για ερευνητικούς σκοπούς, αλλά καθορίζοντας ταυτόχρονα και τις προϋποθέσεις για την προστασία της ιδιωτικότητας, με τεχνικές ανωνυμοποίησης και καταγραφή των δεδομένων εντός του νοσηλευτικού ιδρύματος. Αντίστοιχες δυνατότητες δίνονται και σε γιατρούς όταν αυτοί επιθυμούν να χρησιμοποιήσουν δεδομένα του ιατρικού τους αρχείου για την παραγωγή μιας επιστημονικής δημοσίευσης. Σε αυτή την περίπτωση, η χρήση ιατρικών δεδομένων με τέτοιο τρόπο ώστε να μην είναι αμέσως ή εμμέσως προσδιορίσιμη η ταυτότητα των

ασθενών, δεν συνιστά επεξεργασία προσωπικών δεδομένων. (Παναγοπουλου & Κουτνατζη, 2015)

Σε σχέση με την εγκατάσταση κλειστών κυκλωμάτων τηλεόρασης (CCTV) σε νοσηλευτικά ιδρύματα πρόσφατα ο Υπεύθυνος Προστασίας Δεδομένων του Υπουργείου Υγείας γνωμοδότησε ενάντια, ακόμη και εν μέσω των ειδικών συνθηκών που επικρατούν στην παγκόσμια κοινότητα λόγω της πανδημίας του COVID-19. Οι λόγοι της αρνητικής γνωμοδότησης είναι ότι καταρχήν είναι ενάντιο στις διατάξεις 5 & 9 του GDPR αλλά και με την ΠΝΠ 25/2/2020, οι οποίες μόνο κατ' εξαίρεση επιτρέπουν την εγκατάσταση τέτοιων συστημάτων και μόνο για την παροχή υπηρεσιών υγείας. Μάλιστα, το αίτημα των νοσοκομείων ήταν εγκατάσταση εκτός των θαλάμων και σε κοινόχρηστους χώρους όπως θάλαμοι, κυλικεία και χώροι εστίασης. Και σε αυτό το σημείο η γνωμοδότηση ήταν αρνητική καθώς επιτρέπεται η εγκατάσταση τέτοιων συστημάτων μόνο σε ειδικούς χώρους (πχ ταμεία) και σε άλλους κρίσιμους χώρους όπου δεν επιτρέπεται ούτως ή άλλως η πρόσβαση επισκεπτών. Η συγκεκριμένη διάταξη δεν παύει να ισχύει ούτε για τους σκοπούς της ιχνηλασιμότητας των επισκεπτών που ήρθαν σε επαφή με ασθενείς του COVID-19. Συμπεραίνουμε ότι ακόμα και σε μια ιδιαίτερα απαιτητική εποχή στον τομέα της υγείας όπου πολλοί πολίτες αισθάνονται ότι τα δικαιώματά τους καταπατούνται, ο νόμος είναι σαφής και η τήρησή του επιτρέπει τη διασφάλιση της ιδιωτικότητας ειδικά στους χώρους υγείας. (Lawspot, 2020)

2.2.3 Big data και Υγεία στην Ελλάδα

Τα ιατρικά δεδομένα στην Ελλάδα συγκεντρώνονται – όπως και σε όλο τον κόσμο – σε μεγάλες ποσότητες δεδομένων καταλήγοντας στην ανάγκη χρήσης τεχνολογιών Big Data. Τα ιατρικά δεδομένα προέρχονται από διάφορες πηγές μεταξύ άλλων: συστήματα ιατρικού φακέλου, συστήματα νοσοκομείων, δεδομένα ασφαλιστικών οργανισμών, δημογραφικές και επιδημιολογικές εγγραφές, δεδομένα ιατρικών συσκευών και φαρμάκων, δεδομένα βιοϊατρικών μετρήσεων, βάσεις γενετικών δεδομένων, χρηματοοικονομικές συναλλαγές που σχετίζονται με ιατρική δραστηριότητα, αναζητήσεις διαδικτύου σχετικές με την υγεία, σχετικές αναρτήσεις στα μέσα κοινωνικής δικτύωσης και τέλος αδόμητα δεδομένα αλληλογραφίας. Τα βασικά πληφοροφιακά

συστήματα υγείας από τα οποία συλλέγονται δεδομένα Big Data είναι το Σύστημα Ηλεκτρονικής Συνταγογράφησης (συνταγές φαρμάκων, διαγνωστικών κ.α.) το Σύστημα Πρωτοβάθμιας Υγείας και τα Πληροφοριακά Συστήματα των Νοσοκομείων. Επιπλέον στο σύστημα Ηλεκτρονικής Διακυβέρνησης Κοινωνικής Ασφάλισης (ΗΔΙΚΑ) υπάρχουν περαιτέρω δεδομένα που αφορούν σε πληροφορίες σχετικές με την υγεία όπως κοινωνικό εισόδημα αλληλεγγύης, προνοιακά επιδόματα, επίδομα τέκνου, αναπηρικά επιδόματα κ.α.

Το Σύστημα Ηλεκτρονικής Συνταγογράφησης είναι ίσως η σημαντικότερη πηγή Big Data υγείας, εξαιτίας του όγκου των εμπλεκόμενων φορέων που περιλαμβάνει 50000 πιστοποιημένους γιατρούς και 12800 πιστοποιημένα φαρμακεία ενώ διενεργούνται κάθε μήνα περίπου 6 εκατομμύρια συνταγές και εξυπηρετούνται 3 εκατομμύρια ασφαλισμένοι. Από την έναρξη της λειτουργίας του συστήματος έχουν εκτελεστεί περίπου 550 εκατομμύρια συνταγές φαρμάκων. (Ναυτεμπορική, 2019)

Ο Ηλεκτρονικός Φάκελος Υγείας περιλαμβάνει δεδομένα που (α) καταχωρούνται από τους ιατρούς, (β) προέρχονται από την ηλεκτρονική συνταγογράφηση και (γ) προέρχονται από νοσηλεία σε νοσοκομεία. Στα βασικά στοιχεία περιλαμβάνονται τα στοιχεία του ασθενούς, το ΑΜΚΑ του ιατρού, οι ημερομηνίες επισκέψεων σε ιατρούς και νοσηλευτικές μονάδες. Επιπρόσθετα περιέχονται δεδομένα από το οικογενειακό ιστορικό όπως παθήσεις συγγενών, ατομικό ιστορικό (κοινωνικές συνήθειες όπως τσιγάρο, νοσήματα, ιστορικό εγκυμοσύνης κ.α.) και άλλα στοιχεία όπως εμβόλια, αλλεργίες, εισαγωγές στα νοσοκομεία κ.α. (Αλουγδέλη, 2016)

2.3 Γερμανία

2.3.1 Γενικά

Από την 25η Μαΐου 2018, η βασική νομοθεσία για την προστασία των δεδομένων στην Ευρωπαϊκή Ένωση μέλος της οποίας είναι η Γερμανία είναι ο κανονισμός (ΕΕ) 2016/679 (General Data Protection Regulation – GDPR). Ο κανονισμός αυτός αντικατέστησε την οδηγία 95/46/EC (Data Protection Directive) και οδήγησε σε αυξημένη (αν και όχι συνολική) εναρμόνιση της νομοθεσίας περί προστασίας δεδομένων σε όλα τα κράτη μέλη της ΕΕ. (European Law, 2016)

Ο κανονισμός GDPR ισχύει για επιχειρήσεις που είναι εγκατεστημένες σε οποιοδήποτε κράτος μέλος της ΕΕ όταν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα (ανεξάρτητα αν η επεξεργασία πραγματοποιείται στην ΕΕ ή όχι). Μια επιχείρηση που δεν είναι εγκατεστημένη σε κάποιο κράτος μέλος, αλλά υπόκειται στους νόμους ενός κράτους μέλους δυνάμει του δημοσίου διεθνούς δικαίου, υπόκειται επίσης στον GDPR. Ο GDPR ισχύει για επιχειρήσεις εκτός της ΕΕ εάν επεξεργάζονται τα προσωπικά δεδομένα των κατοίκων της ΕΕ σε σχέση με: (i) την προσφορά αγαθών ή υπηρεσιών (ανεξάρτητα από το αν είναι επί πληρωμή ή όχι) σε κατοίκους της ΕΕ ή (ii) την παρακολούθηση της συμπεριφοράς των κατοίκων της ΕΕ (όταν αυτή η συμπεριφορά λαμβάνει χώρα εντός της ΕΕ). Επιπλέον, ο GDPR ισχύει για επιχειρήσεις εγκατεστημένες εκτός ΕΕ εάν παρακολουθούν τη συμπεριφορά των κατοίκων της ΕΕ (όταν πάλι αυτή η συμπεριφορά λαμβάνει χώρα εντός της ΕΕ). (ICLG, 2020)

Η Γερμανία ενσωμάτωσε τον κανονισμό του GDPR μέσω του Ομοσπονδιακού Νόμου περί Προστασίας Δικαιωμάτων (Bundesdatenschutzgesetz) (Gesetze, 2020), μέσω ελαφρών τροποποιήσεων σε σχέση πχ με τα δικαιώματα στον τομέα της εργασίας και τις καταγραφές CCTV. Επιπρόσθετα υπάρχουν πολλές νομοθετικές πράξεις που περαιτέρω προστατεύουν την ιδιωτικότητα των δεδομένων που σχετίζονται με τις τηλεπικοινωνίες, τις υπηρεσίες διαδικτύου, την υγειονομική περίθαλψη κ.α. Η Γερμανία έχει μια ομοσπονδιακή προσέγγιση στην αρχή προστασίας δεδομένων, επομένως, κάθε γερμανικό κρατίδιο έχει τη δική του αρχή προστασίας δεδομένων. Η ομοσπονδιακή αρχή προστασίας δεδομένων είναι υπεύθυνη για τους ομοσπονδιακούς δημόσιους φορείς και για τις τηλεπικοινωνίες. Επιπλέον, οι εκκλησίες έχουν τις δικές τους εποπτικές αρχές και υπάρχει μια ανεξάρτητη αρχή για τους τηλεοπτικούς και ραδιοφωνικούς φορείς. (ICLG, 2020)

2.3.2 Ψηφιακή Υγεία

Η γερμανική νομοθεσία δεν ορίζει τον όρο «ψηφιακή υγεία». Γενικά, ο όρος είναι αρκετά ευρύς και καλύπτει όλα τα χαρακτηριστικά της υποδομής ψηφιακής υγείας, και συμπεριλαμβάνει: ηλεκτρονικά αρχεία υγείας και ασθενών, ηλεκτρονικές συνταγές φαρμάκων, συστήματα βοήθειας και επιτήρησης υγειονομικής περίθαλψης, υπηρεσίες

τηλεϊατρικής, εξ αποστάσεως ιατρική συμβουλευτική και θεραπεία, εφαρμογές κινητών και φορετών (wearables) συσκευών, εφαρμογή και χρήση βάσεων δεδομένων υγειονομικής περίθαλψης, χρήση τεχνητής νοημοσύνης (AI). Οι βασικές αναδυόμενες τεχνολογίες στον τομέα της ψηφιακής υγείας στη Γερμανία είναι τα λογισμικά ως ιατρικές συσκευές (Software as Medical Device – SaMD), που σε συνδυασμό με τις φορετές συσκευές παρέχουν ιατρική περίθαλψη εξ' αποστάσεως. (ICLG, 2020b)

Οι αρμόδιες γερμανικές δημόσιες αρχές εργάζονται επί του παρόντος για την υλοποίηση μιας λειτουργικής ψηφιακής υποδομής εντός των επόμενων ετών. Όλοι οι πάροχοι υγειονομικής περίθαλψης θα είναι υποχρεωμένοι να συνδεθούν και να προσφέρουν τέτοιες υπηρεσίες στους ασθενείς τους μέσω της υποδομής αυτής. Η πρόκληση είναι η παροχή μιας λειτουργικής και ασφαλούς ψηφιακής υποδομής το συντομότερο δυνατό. Τα θεμελιώδη δικαιώματα της αυτονομίας και της ιδιωτικότητας των ασθενών πρέπει να γίνονται σεβαστά. αλλά πρέπει επίσης να διασφαλιστούν υψηλά πρότυπα υπηρεσιών υγείας. Το γερμανικό κοινοβούλιο και οι αρμόδιες αρχές καλούνται να βρουν μια ισορροπία μεταξύ της χρήσης ψηφιακής υγείας για τη βελτίωση των υπηρεσιών υγειονομικής περίθαλψης, αφενός, και της εφαρμογής επαρκών κανονισμών, αφετέρου, για την προστασία της ανθρώπινης ζωής, της υγείας και το δικαίωμα της ιδιωτικότητας των δεδομένων των ασθενών. (ICLG, 2020b)

2.3.3 Κανονισμοί

Οι πιο σχετικοί κανονισμοί για την παροχή ψηφιακής υγειονομικής περίθαλψης είναι οι τροποποιήσεις των εθνικών και ευρωπαϊκών διατάξεων περί νοσηλείας (π.χ. στα νοσοκομεία) και περίθαλψης εξωτερικών ασθενών (π.χ. γενική ιατρική, παροχή οικιακής φροντίδας). Άλλοι σχετικοί κανονισμοί στον τομέα της ψηφιακής υγειονομικής περίθαλψης είναι οι πρόσφατα τροποποιημένες κρατικές επαγγελματικές διατάξεις για ιατρούς (π.χ. άδεια για εξ' αποστάσεως ιατρική περίθαλψη), νόμοι για επαγγελματική ευθύνη (π.χ. ευθύνη για σωματικούς τραυματισμούς, ζημιές ή οικονομικές απώλειες που προκαλούνται από μια συσκευή που δεν λειτουργεί σωστά), νόμοι περί πνευματικής ιδιοκτησίας (π.χ. προστασία για συστήματα παρακολούθησης με αισθητήρες, όπως σε περιβάλλοντα βρέφους), καθώς και φαρμακευτικοί νόμοι και κανονισμοί για τα φάρμακα

(π.χ. διανομή φαρμάκων μετά από διαδικτυακή ιατρική συμβουλευτική). Επιπρόσθετα, οι εμπορικές συσκευές ρυθμίζονται κυρίως από τον ευρωπαϊκό και εθνικό νόμο περί ιατροτεχνολογικών προϊόντων, τους νόμους περί περίθαλψης εξωτερικών ασθενών (συμπεριλαμβανομένων και κανόνων αποζημίωσης) και τους ευρωπαϊκούς και εθνικούς νόμους περί προστασίας δεδομένων. (ICLG, 2020b)

Στη Γερμανία αυτοδιοικούμενοι σύλλογοι παρόχων υγειονομικής περίθαλψης, όπως οι ομοσπονδιακοί και κρατικοί σύλλογοι δημόσιας υγείας και ασφάλισης (SHI), αδειοδοτημένοι ιατροί, ο Οργανισμός ιδιωτικών ασφαλιστών υγειονομικής περίθαλψης και ο ομοσπονδιακός και κρατικός Οργανισμός των ασφαλιστών υγειονομικής περίθαλψης, εξουσιοδοτούνται από το νόμο για αυτόνομη ρύθμιση και καθορισμό σημείων του τομέα της υγειονομικής περίθαλψης μέσω καταστατικών, κατευθυντήριων γραμμών και δευτερογενών κανονισμών. Οι αυτοδιοικούμενες αυτές οντότητες είναι μαζί με το Υπουργείο Υγείας, οι συμμετέχοντες στην Gesellschaft für Telematik (Gematik).

Η Gematik είναι μια ειδικού σκοπού και τύπου εταιρεία την οποία η σχετική γερμανική νομοθεσία έχει εμπιστευτεί να αναπτύξει την κατάλληλη τεχνική υποδομή για την ηλεκτρονική κάρτα υγείας ασθενούς, τα ηλεκτρονικά αρχεία ασθενών, την ηλεκτρονική συνταγογράφηση φαρμάκων και άλλες ηλεκτρονικές εφαρμογές και χαρακτηριστικά που θα είναι άμεσα ή στο μέλλον διαθέσιμα στον τομέα της υγειονομικής περίθαλψης στη Γερμανία. Η Gematik είναι επίσης υπεύθυνη για την κατασκευή και τη συντήρηση της απαιτούμενης υποδομής τηλεματικής, καθώς και για την εγγραφή όλων των παρόχων υγειονομικής περίθαλψης στην υποδομή εντός καθορισμένου χρονικού πλαισίου.

Από την 1η Ιανουαρίου 2020, οι ασθενείς που είναι εγγεγραμμένοι στην ασφάλιση SHI δικαιούνται συνταγογράφηση για όσες εφαρμογές ψηφιακής υγειονομικής περίθαλψης καταχωρίστηκαν από το Ομοσπονδιακό Ινστιτούτο Φαρμάκων και Ιατρικών Συσκευών (BfArM) ενώ οι δαπάνες που θα πραγματοποιήσουν είναι επιστρέψιμες. Η υποχρέωση καταχώρησης στο προαναφερθέν ινστιτούτο από τις ψηφιακές εφαρμογές υγειονομικής περίθαλψης είναι ένας βασικός τρόπος επιβολής κανόνων και ελέγχου των

υπηρεσιών εξ' αποστάσεως περίθαλψης, πάντα σε σχέση και με την προστασία ευαίσθητων προσωπικών δεδομένων υγειονομικής περίθαλψης.

Ένα ιατρικό λογισμικό, υπό ορισμένες προϋποθέσεις, θεωρείται ιατροτεχνολογικό προϊόν και επομένως υπόκειται στις απαιτήσεις των οδηγιών περί ιατροτεχνολογικών προϊόντων της ΕΕ και στη σχετική νομοθεσία των κρατών μελών. Επομένως, προτού διατεθεί ένα λογισμικό ως ιατροτεχνολογικό προϊόν (SaMD) στην αγορά της ΕΕ πρέπει να υποβληθεί σε διαδικασία αξιολόγησης για να επιβεβαιωθεί ότι συμμορφώνεται με τις βασικές απαιτήσεις της Οδηγίας Ιατρικών Συσκευών της ΕΕ (MDD). Ο τρόπος της διαδικασίας αξιολόγησης της συμμόρφωσης που χρησιμοποιείται εξαρτάται από την κατηγορία και το επίπεδο κινδύνου του αναμένεται να έχει το εν λόγω προϊόν. Επί του παρόντος, το μεγαλύτερο ποσοστό των SaMD κατατάσσεται στην κατηγορία I και επομένως υπόκειται στη βασική διαδικασία αξιολόγησης της συμμόρφωσης που δεν απαιτεί τη συμμετοχή ενός πιστοποιημένου οργανισμού. Μετά την επιτυχή ολοκλήρωση της αξιολόγησης συμμόρφωσης, ο κατασκευαστής μπορεί να τοποθετήσει το σήμα CE στο προϊόν. Το σήμα CE επιτρέπει στον κατασκευαστή να διαθέσει το προϊόν στην αγορά στη ζώνη CE, η οποία καλύπτει επί του παρόντος τον ΕΟΧ (ΕΕ και χώρες Ελεύθερης ζώνης ΕΖΕΣ), καθώς και την Τουρκία και την Ελβετία. (Schnell-Inderst et al., 2015)

Το 2017, εγκρίθηκαν οι νέοι κανονισμοί της ΕΕ για τα ιατροτεχνολογικά προϊόντα. Το νέο καθεστώς τέθηκε σε ισχύ στις 27 Μαΐου 2020 (για ιατροτεχνολογικά προϊόντα) και στις 27 Μαΐου 2022 (για διαγνωστικά ιατροτεχνολογικά προϊόντα). Το νέο νομικό πλαίσιο τροποποιεί το σύστημα ταξινόμησης κινδύνων και ως αποτέλεσμα πολλές συσκευές θα ταξινομηθούν σε κατηγορίες υψηλότερου κινδύνου. Λόγω αυτής της διαφορετικής ταξινόμησης, αλλά και ως αποτέλεσμα των αυξημένων απαιτήσεων στη διαδικασία αξιολόγησης της συμμόρφωσης, η διάθεση ιατρικών συσκευών στην αγορά της ΕΕ αναμένεται να γίνει πιο δύσκολη. Τα περισσότερα προϊόντα SaMD ταξινομούνται επί του παρόντος στην κλάση I, αν και υπάρχει κίνδυνος αύξησης της ταξινόμησής τους. Κατά συνέπεια, βάσει του νέου νόμου, οι κατασκευαστές SaMD θα χρειάζονται πιο συχνά πλέον πιστοποιητικά CE που εκδίδονται από πιστοποιημένου οργανισμούς σε σχέση με το παρελθόν.

2.3.4 Προστασία δεδομένων

Τα προσωπικά δεδομένα ρυθμίζονται κατά κύριο λόγο από τον GDPR. Σύμφωνα με τον GDPR, κάθε εμπλεκόμενος στη διαδικασία, δηλαδή καθένας που καθορίζει τον σκοπό και τα μέσα της επεξεργασίας δεδομένων (άρθρο 4 αριθ. 7 GDPR), είναι υπεύθυνος για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με όλους τους σχετικούς νόμους περί προστασίας δεδομένων. Στο πλαίσιο της ψηφιακής υγείας, υπάρχουν συχνά περισσότεροι από ένας υπεύθυνοι επεξεργασίας δεδομένων, καθώς λόγω της πολυποικιλότητας του είδους και της μορφής των ιατρικών δεδομένων, εμπλέκονται περισσότεροι από ένας φορείς. Οι υπεύθυνοι επεξεργασίας δεδομένων βάσει του GDPR μπορούν να είναι πάροχοι υπηρεσιών υγειονομικής περίθαλψης, πάροχοι των σχετικών πλατφορμών ή εταιρείες που χρησιμοποιούν εφαρμογές υγειονομικής περίθαλψης για εκμετάλλευση των υπηρεσιών τους. (European Law, 2016)

Σύμφωνα με το GDPR και τους πρόσθετους σχετικούς γερμανικούς νόμους περί προστασίας δεδομένων (όπως Γερμανικός Ομοσπονδιακός Κώδικας για την Προστασία Δεδομένων (BDSG)), τα δεδομένα υγείας και ασθενών ανήκουν στις ειδικές κατηγορίες προσωπικών δεδομένων. Σύμφωνα με από το άρθρο. 9 παρ. 1 του GDPR, απαγορεύεται η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων, εκτός αν η επεξεργασία δικαιολογείται από το νόμο, (κυρίως το άρθρο. 9 παρ. 2 h και g) ή με τη συγκατάθεση του ατόμου από το οποίο πηγάζουν τα δεδομένα. Επιπλέον, πρέπει να ελέγχεται η εφαρμογή του δικαιώματος του ασθενούς να διατηρεί την εμπιστευτικότητα της σχέσης του με το γιατρό, καθώς και τα σχετικά δεδομένα που αυτός επεξεργάζεται. (European Law, 2016)

Η “ψηφιακή υγεία” επηρεάζει περισσότερα άτομα και φορείς από τον παραδοσιακό τρόπο υγειονομικής περίθαλψης καθώς εμπλέκονται εκτός του ασθενή, του υγειονομικού επαγγελματία και των ρυθμιστικών αρχών και άλλα συχνά μη σχετικά με τον ιατρικό τομέα μέρη, όπως πχ ο πάροχος της πλατφόρμας (big data, cloud) ή ο προγραμματιστής της ψηφιακής εφαρμογής. Ωστόσο, με βάση τη γερμανική νομοθεσία η απελευθέρωση της χρήσης και επεξεργασίας προσωπικών δεδομένων απαιτεί τη συμμετοχή μερών που δεσμεύονται από επαγγελματικές υποχρεώσεις εμπιστευτικότητας

(π.χ. γιατροί, νοσηλευτές, ασφαλιστές υγείας κ.α.). Οι ενδιαφερόμενοι που δεν προέρχονται από το χώρο της υγείας και επομένως δεν περιορίζονται από τους κανόνες τις εμπιστευτικότητας, μπορούν να επεξεργαστούν δεδομένα υγειονομικής περίθαλψης μόνο εφόσον υπάρχει πρότερη και ενημερωμένη συναίνεση των ασθενών. Αυτή η απαίτηση μπορεί να δημιουργήσει οργανωτικές δυσκολίες, π.χ. σε περίπτωση βάσεων δεδομένων ή όταν υποβάλλονται σε επεξεργασία τεράστιες ποσότητες δεδομένων υγείας, καθώς οι ασθενείς των δεδομένων μπορούν να ανακαλέσουν τη συγκατάθεσή τους ανά πάσα στιγμή. Έτσι η επεξεργασία των Big Data είναι ιδιαίτερα προβληματική και δύσκολη σε σχέση με τους νομικούς περιορισμούς που υπάρχουν. (ICLG, 2020b)

2.3.5 IoT και Cloud

Στη Γερμανία, οι οργανισμοί υγειονομικής περίθαλψης που μεταφέρουν μέρος των λειτουργιών τους στο «νέφος» προκειμένου να μειώσουν το κόστος και να βελτιώσουν την προσβασιμότητα και τη διαχείριση των δεδομένων των ασθενών αντιμετωπίζουν νομικές, ιατρικές, τεχνικές, οργανωτικές και οικονομικές προκλήσεις. Η ασφάλεια και η εμπιστευτικότητα είναι βασικές πτυχές για την ευρεία χρήση υπηρεσιών που βασίζονται σε cloud. Για να μειώσουν τον κίνδυνο επιθέσεων στον κυβερνοχώρο και την απώλεια ευαίσθητων δεδομένων, οι οργανισμοί υγειονομικής περίθαλψης πρέπει να διασφαλίσουν ένα ασφαλές σύστημα για τη μεταφορά, τη συντήρηση και τη λήψη ευαίσθητων πληροφοριών για την υγεία. Ωστόσο, πρέπει να διασφαλιστεί η διαλειτουργικότητα μεταξύ των συνεργατών, καθώς και ένα σύστημα διαχείρισης που επιτρέπει πολλαπλή αλλά ασφαλή πρόσβαση σε σχετικά δεδομένα. Η εμπιστευτικότητα μπορεί να επιτευχθεί με τον έλεγχο πρόσβασης και χρησιμοποιώντας τεχνικές κρυπτογράφησης. Σε νομικό επίπεδο, πρέπει να τηρούνται οι απαιτήσεις προστασίας δεδομένων, όπως η υποχρέωση ανταλλαγής ανωνυμοποιημένων δεδομένων. (ICLG, 2020)

Οι μη υγειονομικές εταιρείες δεν επιτρέπεται να παρέχουν ιατρικές υπηρεσίες σε ασθενείς. Οι ιατρικές υπηρεσίες προορίζονται για επαγγελματικά εκπαιδευμένο προσωπικό όπως γιατρούς, άλλους επαγγελματίες υγείας και ιδιωτικές εταιρείες υγειονομικής περίθαλψης με άδεια για αυτές τις υπηρεσίες. Οι εταιρείες μη υγειονομικής

περίθαλψης μπορούν να υποστηρίξουν επαγγελματίες υγείας που παρέχουν σε αυτούς ή στους ασθενείς τους επικουρικές μη ιατρικές υπηρεσίες. Εντούτοις, οι εταιρείες μη υγειονομικής περίθαλψης μπορούν να διανέμουν ιατρικές συσκευές όπως εφαρμογές υγειονομικής περίθαλψης. Μόνο λοιπόν η εμπορική διανομή ιατρικών συσκευών επιτρέπεται σε όλους και δεν περιορίζεται σε επαγγελματίες υγείας.

Καταλήγοντας, ο τομέας της ψηφιακής υγείας είναι ένας αρκετά νέος και πολύπλοκος τομέας που αναπτύσσεται ταχύτατα στη Γερμανική αγορά. Το υπουργείο υγείας της Γερμανίας τα τελευταία χρόνια άρχισε να εξετάζει συστηματικά το ζήτημα της μεταρρύθμισης των γερμανικών νόμων περί υγειονομικής περίθαλψης, εισάγοντας και καθιερώνοντας βήμα προς βήμα τηλε-ιατρικές υπηρεσίες, συμπεριλαμβανομένης της επιστροφής δαπανών, στην τυπική ιατρική περίθαλψη. Αυτό δείχνει ότι ο γερμανικός τομέας ψηφιακής υγείας δεν έχει ακόμη ρυθμιστεί πλήρως, καθώς ακόμα υπάρχουν μόνο ορισμένοι ειδικοί νόμοι και διατάξεις που τον διέπουν. Για τις εταιρείες που δεν συγκαταλέγονται στον τομέας της υγειονομικής περίθαλψης, αυτό μπορεί να είναι, αφενός, ένα πλεονέκτημα επειδή η αγορά ψηφιακής υγειονομικής περίθαλψης είναι ανοιχτή σε νέες ιδέες και ανάπτυξη. Από την άλλη πλευρά, η αγορά υγειονομικής περίθαλψης είναι πολύ ευαίσθητη (δεδομένου του θεμελιώδους δικαιώματος στη ζωή και την υγεία) και συντηρητική (οι επαγγελματίες υγείας στη Γερμανία διαθέτουν ισχυρό λόμπι). Αυτό ενέχει τον κίνδυνο ότι η γερμανική αγορά υγειονομικής περίθαλψης δεν θα αναπτυχθεί τόσο γρήγορα όσο επιθυμούν οι εταιρείες. Παρ' όλ' αυτά, η διαδικασία ενσωμάτωσης καινοτομίας στη γερμανική ιατρική περίθαλψη έχει ξεκινήσει και δύσκολα θα περιοριστεί. (Kleine, 2018)

2.4 ΗΠΑ

2.4.1 Νομοθεσία

Το πλαίσιο προστασίας προσωπικών δεδομένων για την υγεία στις ΗΠΑ είναι ένα σύνολο ομοσπονδιακών και πολιτειακών νόμων που συχνά αλληλεπικαλύπτονται και ρυθμίζουν συγκεκριμένους τύπους πληροφοριών, ατόμων και οργανισμών. Η σύγχυση που σχετίζεται με το πεδίο εφαρμογής και την εφαρμογή αυτού του πλαισίου, καθώς και

η πολυπλοκότητα των νόμων, έχει δυσκολέψει την εφαρμογή των Big Data στην υγεία. Συνολικά πάντως, το πλαίσιο επιτρέπει πολλών ειδών χρήσεις δεδομένων που είναι ευεργετικές για τη δημόσια υγεία. Παρακάτω αναλύονται οι βασικοί ομοσπονδιακοί νόμοι.

Νόμος Health Information Portability and Accountability Act του 1996 (HIPAA). Ο κανονισμός απορρήτου του HIPAA κατοχυρώνει τις «προστατευόμενες πληροφορίες σχετικές με την υγεία» οι οποίες περιλαμβάνουν πληροφορίες σχετικά με τη ιατρική περίθαλψη ενός ατόμου, την κατάσταση της υγείας του ή σχετικές πληρωμές σε φορείς που πραγματοποίησε. Ο κανονισμός δεν ισχύει σε πληροφορίες οι οποίες είναι ανωνυμοποιημένες, πληροφορίες από τις οποίες έχουν αφαιρεθεί συγκεκριμένα αναγνωριστικά ή που κάποιος εμπειρογνώμονας έχει αποφανθεί ότι οι πληροφορίες περιέχουν ελάχιστο κίνδυνο να χρησιμοποιηθούν ώστε να ταυτοποιηθεί το άτομο στο οποίο αναφέρονται. Ο Κανόνας απορρήτου ισχύει για όλες τις «συμμετέχουσες οντότητες» (δηλ. προγράμματα υγείας, πάροχοι υγειονομικής περίθαλψης κλπ) και τους «συνεργάτες τους» (δηλαδή, οντότητες που έχουν πρόσβαση ή χρησιμοποιούν προστατευόμενες πληροφορίες σχετικές με την υγεία κατά την εκτέλεση συγκεκριμένων λειτουργιών ή υπηρεσιών). (HHS, 2020)

Οι ανωτέρω ρυθμιζόμενες οντότητες υποχρεούνται να αποκαλύπτουν «προστατευόμενες πληροφορίες σχετικές με την υγεία» στο άτομο που ανήκουν οι πληροφορίες ή σε εξουσιοδοτημένο εκπρόσωπό του αλλά και στο Γραμματέα του Υπουργείου Υγείας και Ανθρωπίνων Υπηρεσιών των ΗΠΑ για σκοπούς έρευνας. Οι ρυθμιζόμενες οντότητες ενδέχεται να αποκαλύπτουν μέρος αυτών των πληροφοριών σε οποιονδήποτε άλλο με τη συγκατάθεση του ατόμου και επιτρέπεται (αλλά δεν απαιτείται) να αποκαλύπτουν τις πληροφορίες αυτές χωρίς συναίνεση αν ισχύει κάποια από τις παρακάτω εξαιρέσεις:

- *Θεραπεία, πληρωμές και λειτουργία*. Γενικά, οι ρυθμιζόμενες οντότητες μπορούν να αποκαλύπτουν προστατευόμενες πληροφορίες υγείας χωρίς άδεια για θεραπευτικούς σκοπούς (π.χ. παράδοση φροντίδας ασθενών), δραστηριότητες πληρωμής (π.χ. πληρωμή για υπηρεσίες) και λειτουργίες υγειονομικής περίθαλψης (π.χ. ενέργειες βελτίωσης της ποιότητας)

- *Δραστηριότητες δημόσιας υγείας*. Οι ρυθμιζόμενες οντότητες μπορούν να αποκαλύπτουν προστατευόμενες πληροφορίες υγείας χωρίς άδεια σε νομικά εξουσιοδοτημένους φορείς δημόσιας υγείας για σκοπούς που σχετίζονται με την πρόληψη ή τον έλεγχο ασθενειών, τραυματισμού ή αναπηρίας (π.χ. παρακολούθηση ασθενειών). Ο Κανονισμός απορρήτου γενικά προσδιορίζει έξι δημόσιες υγειονομικές δραστηριότητες για τις οποίες επιτρέπεται η αποκάλυψη, συμπεριλαμβανομένων μεταξύ άλλων περιπτώσεων μεταδοτικών ασθενειών και περιπτώσεων που εμπλέκονται σχολικά περιβάλλοντα.
- *Άλλες εξαιρέσεις*. Ο Κανονισμός απορρήτου προσδιορίζει 11 άλλους σκοπούς για τους οποίους μπορεί να γίνει αποκάλυψη χωρίς άδεια. Αυτές οι εξαιρέσεις περιορίζονται σε συγκεκριμένες δραστηριότητες που είναι επωφελείς για το κοινό και περιλαμβάνουν ενέργειες όπως προστασία της εθνικής ασφάλειας, επιβολή του νόμου και έρευνα μόνο για συγκεκριμένους σκοπούς.
- *Περιορισμένα σύνολα δεδομένων*. Οι ρυθμιζόμενες οντότητες επιτρέπεται να αποκαλύπτουν ένα περιορισμένο σύνολο δεδομένων χωρίς άδεια για έρευνα, δημόσια υγεία ή λειτουργίες υγειονομικής περίθαλψης. Ένα περιορισμένο σύνολο δεδομένων περιέχει το αρχικό σύνολο δεδομένων χωρίς 16 καθορισμένα αναγνωριστικά, (μπορεί εντούτοις να περιλαμβάνει πόλη, πολιτεία και ταχυδρομικό κώδικα, ημερομηνίες και χαρακτήρες ή κωδικούς που δεν είναι άμεσα αναγνωριστικά). Τα συνεργαζόμενα μέρη που ανταλλάσσουν το σύνολο δεδομένων πρέπει να συνάψουν συμφωνία χρήσης δεδομένων που διέπει τη χρήση του περιορισμένου συνόλου δεδομένων. (HHS, 2020)

Ο Κοινός Κανόνας. Ο Κοινός Κανόνας προστατεύει τα άτομα που εμπλέκονται σε έρευνα που χρηματοδοτείται σε ομοσπονδιακό επίπεδο καθώς και ευαίσθητες πληροφορίες που σχετίζονται με ένα άτομο, απαιτώντας γενικά είτε έγκριση από πιστοποιημένο οργανισμό (Institutional review board - IRB) και συγκατάθεση ασθενούς είτε απόρριψη από το IRB της απαίτησης συγκατάθεσης. Ο Κοινός Κανόνας δεν ισχύει για τις έρευνες που διεξάγονται με χρήση υπαρχουσών πληροφοριών ασθενούς, με παρατήρηση δημόσιας συμπεριφοράς, ή με διαδικασίες έρευνας μέσω συνέντευξης. Ο Κοινός Κανόνας εξαιρεί επίσης μελέτες που χρησιμοποιούν υπάρχοντα δεδομένα, αρχεία

ή βιο-δείγματα εάν τα αποτελέσματα δεν αποκαλύπτουν την ταυτότητα του υποκειμένου ή εάν οι πηγές δεδομένων είναι δημόσια διαθέσιμες. (Burris, & Puglisi, 2018)

Νόμος Genetic Information Nondisclosure Act του 2008 (GINA). Ο GINA απαγορεύει γενικά σε προγράμματα και πλάνα υγείας να χρησιμοποιούν γενετικές πληροφορίες για να λαμβάνουν αποφάσεις σχετικές με υγειονομική κάλυψη ή να ζητούν από τους δικαιούχους να υποβληθούν σε γενετικούς ελέγχους ή να παρέχουν γενετικές πληροφορίες. Ο GINA απαγορεύει επίσης γενικά σε εργοδότες να κάνουν διακρίσεις εις βάρος υπαλλήλων ή αιτούντων βάσει γενετικών πληροφοριών και να χρησιμοποιούν γενετικές πληροφορίες στην πρόσληψη και διαχείριση των υπαλλήλων τους, με την επιφύλαξη συγκεκριμένων εξαιρέσεων. Οι εργοδότες μπορούν να αποκαλύψουν γενετικές πληροφορίες σε ορισμένες περιστάσεις, όπως πχ σε ερευνητή ή σε οργανισμό δημόσιας υγείας, εάν οι πληροφορίες σχετίζονται με μεταδοτική ασθένεια που παρουσιάζει απειλή σοβαρής βλάβης ή θανάτου. (Feldman, 2012)

Πολιτειακοί νόμοι και κανονισμοί. Οι πολιτείες ορίζουν το δικό τους πλαίσιο απορρήτου, το οποίο συνήθως περιλαμβάνει νόμους που διέπουν τις ίδιες οντότητες, δραστηριότητες και τύπους πληροφοριών με τους ομοσπονδιακούς νόμους. Γενικά, οι πάροχοι υγειονομικών υπηρεσιών πρέπει να συμμορφώνονται με όλους τους ομοσπονδιακούς νόμους και με όσους πολιτειακούς κανονισμούς είναι πιο αυστηροί. Οι πολιτείες συνήθως προστατεύουν περισσότερο από την ομοσπονδία ευαίσθητες πληροφορίες υγείας (π.χ. πληροφορίες ψυχικής υγείας) και ειδικά για ορισμένους ευάλωτους πληθυσμούς (π.χ. ανήλικοι). Οι νόμοι και οι κανονισμοί των πολιτειών συνήθως περιορίζουν την αποκάλυψη αναγνωρίσιμων πληροφοριών περισσότερο από τους ομοσπονδιακούς νόμους και οι οργανισμοί και φορείς που αποκαλύπτουν ή χρησιμοποιούν αναγνωρίσιμες πληροφορίες υγείας οφείλουν να γνωρίζουν τον τρόπο με τον οποίο η εκάστοτε πολιτεία ρυθμίζει τη διαχείριση των ευαίσθητων πληροφοριών. Επιπλέον, οι πολιτείες συχνά απαιτούν να τους ενημερώνουν με πληροφορίες που σχετίζονται με μεταδοτικές ασθένειες και γενικά υποχρεώνουν την υποβολή δεδομένων και εκθέσεων προς υποστήριξη δραστηριοτήτων δημόσιας παρακολούθησης της υγείας και έρευνας. (Schmit et al., 2018)

2.4.2 Εφαρμογή της νομοθεσίας και Big Data

Η κατανόηση του νομοθετικού πλαισίου για την προστασία της ιδιωτικότητας είναι κρίσιμη για τη χρήση Big Data στον τομέα της υγείας των ΗΠΑ. Ενώ κάθε νόμος επιτρέπει την αποκάλυψη πληροφοριών για την υγεία με τη συγκατάθεση του ασθενούς, η απόκτηση της απαιτούμενης συγκατάθεσης μπορεί να είναι ανέφικτη, ιδίως για δραστηριότητες που βασίζονται σε μεγάλους πληθυσμούς. Υπάρχουν εντούτοις κάποιες εξαιρέσεις που επιτρέπουν την αποκάλυψη πληροφοριών για την υγεία χωρίς συγκατάθεση, επιτρέποντας έτσι δραστηριότητες προς όφελος της δημόσιας υγείας. Οι μη ρυθμιζόμενοι οργανισμοί εκτός του πλαισίου προσφέρουν επίσης ευκαιρίες για την εκμετάλλευση των Big Data.

Εξαιρέσεις για τη δημόσια υγεία. Κάθε ομοσπονδιακός νόμος έχει προβλέψει εξαιρέσεις προς όφελος των βασικών υπηρεσιών δημόσιας υγείας. Οι εξαιρέσεις του νόμου HIPAA επιτρέπουν σε ρυθμιζόμενες οντότητες να αποκαλύπτουν πληροφορίες υγείας χωρίς εξουσιοδότηση για δραστηριότητες που σχετίζονται με την πρόληψη ή τον έλεγχο ασθένειας, τραυματισμού ή αναπηρίας. Παραδοσιακές δραστηριότητες δημόσιας υγείας όπως παρακολούθηση εστίας μιας νόσου, παρακολούθηση της χρήσης ορισμένων φαρμάκων και στόχευση προληπτικών ελέγχων ανήκουν στις εξαιρέσεις του νόμου. Ένα πρόσφατο παράδειγμα είναι μια βάση δεδομένων της Νέας Υόρκης που δημιουργήθηκε από ανώτερους υπαλλήλους της δημόσιας υγείας, η οποία παρακολουθεί την εκταμίευση συνταγογραφούμενων φαρμάκων έτσι ώστε οι πάροχοι να μπορούν να προσδιορίσουν εάν ένα άτομο διαθέτει εν ενεργεία συνταγή. Κατά το πρώτο έτος, η βάση δεδομένων έλαβε επτά εκατομμύρια ερωτήματα από 66.000 παρόχους, μειώνοντας τα έξοδα φαρμακευτικής αγωγής κατά 75%. (Attorney General, 2014)

Οι εξαιρέσεις του νόμου HIPAA για τις επιχειρήσεις υγειονομικής περίθαλψης είναι αρκετά ανεκτικές περιλαμβάνοντας πολλές δραστηριότητες σχετικές με την υγεία του πληθυσμού. Για παράδειγμα, το National Drug Early Warning System, που δημιουργήθηκε από το Κέντρο Substance Abuse Research του Μέριλαντ, παρακολουθεί τα κοινωνικά μέσα αλλά και παραδοσιακές πηγές δεδομένων ώστε με τη χρήση αναλυτικής Big Data να εντοπίζει τις αναδυόμενες τάσεις φαρμάκων, έτσι ώστε η ηγεσία

της δημόσιας υγείας να μπορεί να οργανώσει σχετικές κοινοτικές παρεμβάσεις. (NIH, 2014) Επιπρόσθετα, οι προστατευόμενες πληροφορίες υγείας μπορούν να επιτρέψουν και να ενθαρρύνουν δραστηριότητες βελτίωσης της ποιότητας, όπως αυτές του έργου «Reducing Avoidable Readmissions Effectively (RARE)» της Μινεσότα. Τα νοσοκομεία χρησιμοποιούν αυτές τις πληροφορίες για να αντιμετωπίσουν πιο αποτελεσματικά το φαινόμενο των επανεισαγωγών ασθενών σε κέντρα υγείας. Το έργο RARE απέτρεψε σχεδόν 8.000 επανεισαγωγές. (Rosenbaum, 2016)

Η αποκάλυψη προστατευόμενων πληροφοριών υγείας είναι επιτρεπτή επίσης για δραστηριότητες που σχετίζονται με τη βελτίωση της δημόσιας υγείας ή τη μείωση του κόστους υγειονομικής περίθαλψης. Η διαχείριση της υγείας μεγάλης πληθυσμιακής ομάδας απαιτεί την ταξινόμηση των ασθενών ή προσδιορισμό των υποομάδων που θα επωφεληθούν από συγκεκριμένες στοχευμένες παρεμβάσεις. Η Kaiser Permanente Northern California (KPNC) εφάρμοσε ένα πρόγραμμα για τη βελτίωση του ποσοστού ελέγχου υπέρτασης το οποίο μέχρι τότε μετρούνταν στα επίπεδα του 43,6%. Το πρόγραμμα χρησιμοποίησε δεδομένα από ένα κεντρικό μητρώο για να ταξινομήσει τους ασθενείς, να εντοπίσει σε αυτή λίστα περιπτώσεις που απαιτούν επιπρόσθετη φροντίδα και να ειδοποιήσει τις τοπικές υγειονομικές αρχές για ασθενείς των οποίων η υπέρταση δεν μετρούνταν. Μέσα σε λίγα χρόνια, ο έλεγχος υπέρτασης εντός του KNPC έφτασε το 80,4%. (Jaffe et al., 2013). Τέλος, η επιτυχής διαχείριση της υγείας του πληθυσμού βασίζεται στο συνδυασμό δημογραφικών, συμπεριφορικών και κλινικών δεδομένων για την ανάπτυξη πιο αποτελεσματικών παρεμβάσεων. Στο Πανεπιστήμιο του Duke, οι ερευνητές ενσωμάτωσαν στοιχεία απογραφής, στατιστικές εγκλήματος, στατιστικές στέγασης και περιβαλλοντικά δεδομένα για να υποστηρίξουν έργα δημόσιας υγείας. (Miranda et al., 2013)

2.4.3 Τρέχουσα κατάσταση

Με βάση την προηγούμενη ανάλυση, φαίνεται ότι ο νόμος HIPAA προστατεύει τους Αμερικανούς από το να κοινοποιούνται ή να κλέβονται οι ευαίσθητες πληροφορίες για την υγεία τους αλλά κάτι τέτοιο δεν ισχύει. Νέες μέθοδοι αποθήκευσης και ανταλλαγής δεδομένων έχουν δημιουργήσει κενά στο κανονιστικό πλαίσιο κάτι που μπορούν να

εκμεταλλευτούν όσοι έχουν κακόβουλη πρόθεση. Ομοσπονδιακοί και πολιτειακοί νόμοι που έχουν σχεδιαστεί για την ασφάλεια των προστατευόμενων πληροφοριών υγείας, όπως ο HIPAA, εφαρμόζονται μόνο σε «καλυπτόμενες οντότητες» - παρόχους υγειονομικής περίθαλψης και ερευνητικά ιδρύματα. Δεν επιβάλλονται διεθνώς και κυρίως δεν επιβάλλονται στο Διαδίκτυο. Επιπρόσθετα, η μετάδοση πληροφοριών για την υγεία διεθνώς μεταξύ κρατών βασίζεται σε εθελοντικές συμφωνίες και οι ιδιωτικές εταιρείες μπορούν να ζητούν δεδομένα υγείας από τους χρήστες χωρίς να πρέπει να συμμορφώνονται με τους κανονισμούς HIPAA. (Gostin et al., 2018)

Ως αποτέλεσμα, όλο και περισσότερες προσωπικές πληροφορίες, συμπεριλαμβανομένων των δεδομένων υγείας, συλλέγονται από παρόχους υπηρεσιών Διαδικτύου και τρίτες εταιρείες αναλυτικής για πώληση σε εταιρείες μάρκετινγκ. Η συχνότερη απαίτηση συναίνεσης στο Διαδικτύου ζητείται από τους χρήστες σε έγγραφα όπως «Όροι Παροχής Υπηρεσιών», τα οποία είναι συνήθως πυκνά, πολύπλοκα έγγραφα που δεν διαβάζονται ή δεν κατανοούνται πλήρως. Μια νέα κουλτούρα κοινωνικών μέσων μαζικής ενημέρωσης και ανταλλαγής δεδομένων έχει ενθαρρύνει τους Αμερικανούς να μοιράζονται πρόθυμα προσωπικές πληροφορίες σε διαδικτυακά φόρουμ, τα οποία δεν ρυθμίζονται βάσει του HIPAA. Αυτές οι πληροφορίες μπορεί να μην είναι ιατρικού χαρακτήρα, αλλά μπορούν να χρησιμοποιηθούν για τη σύνδεση ανωνυμοποιημένων ιατρικών δεδομένων με συγκεκριμένα άτομα. (Sitn, 2019)

Μια έρευνα το 2018 έδειξε ότι θα μπορούσαν να πάρουν ένα μεγάλο σύνολο δεδομένων υγείας, να αφαιρέσουν τις «προστατευόμενες πληροφορίες» και να χρησιμοποιήσουν μηχανική μάθηση για να επαναπροσδιορίσουν το 95% των ενηλίκων και το 80% των παιδιών. Κατάφεραν να το κάνουν αυτό εκπαιδεύοντας έναν αλγόριθμο με δημογραφικά δεδομένα και δεδομένα φυσικής κατάστασης (από φορετές συσκευές). Η έρευνα κατέληξε ότι χάρη στον όγκο πληροφορίας που είναι διαθέσιμη δημόσια για ένα συγκεκριμένο άτομο, αυτή η μέθοδος θα μπορούσε να χρησιμοποιηθεί για να προβλέψει την ταυτότητα του ατόμου χρησιμοποιώντας φαινομενικά ανώνυμες πληροφορίες. (Na et al., 2018)

Παρόλο που τα κενά στους κανονισμούς HIPAA δεν έχουν επιτρέψει τη βέλτιστη προστασία της ιδιωτικότητας των πληροφοριών υγείας, υπάρχουν ενέργειες μέσω νομοθεσίας που θα επιτρέψουν να βελτιωθεί ο έλεγχος και η ασφάλεια τους. Νέοι νόμοι από το Κογκρέσο και νέοι κανονισμοί από τις ομοσπονδιακές υπηρεσίες ενδέχεται να επεκτείνουν τις οντότητες που υπόκεινται στη ρύθμιση HIPAA ώστε να συμπεριλάβουν όλες τις οντότητες που συλλέγουν προσωπικές πληροφορίες για την υγεία, συμπεριλαμβανομένων εταιρειών όπως το Facebook και η Google. Τα πρωτόκολλα κρυπτογράφησης και ανωνυμοποίησης θα μπορούσαν να ενημερωθούν για την καταπολέμηση της απειλής της επαναγνώρισης μέσω μηχανικής μάθησης. Τέλος, αυτές οι οντότητες θα μπορούσαν να υποχρεωθούν να αποκαλύψουν σε σαφή γλώσσα πώς θα χρησιμοποιηθούν αυτά τα δεδομένα. Το σίγουρο είναι ότι οι ΗΠΑ έχουν ακόμα αρκετό δρόμο μπροστά τους σε σχέση με την ιδιωτικότητα των δεδομένων υγείας, ειδικά την εποχή των Big Data. (Sitn, 2019)

2.5 Καναδάς

2.5.1 Νομοθεσία για απόρρητο

Χάρη στη ραγδαία αύξηση στους ρυθμούς ανάπτυξης νέων τεχνολογιών ικανών να συλλέγουν και να αποθηκεύουν τεράστιες ποσότητες πληροφοριών, η ιδιωτικότητα στην Καναδική υγειονομική περίθαλψη έχει αναδειχθεί ως κρίσιμο θέμα. Η καναδική νομοθεσία περί προστασίας της ιδιωτικής ζωής στον τομέα της υγείας χωρίζεται σε 14 κυβερνητικές δικαιοδοσίες (η ομοσπονδιακή κυβέρνηση, 10 επαρχίες και 3 περιοχές) η καθεμία με το δικό της νομοθετικό πλαίσιο για την προστασία του απορρήτου των προσωπικών πληροφοριών ή προσωπικών πληροφοριών για την υγεία (PHI).

Υπάρχουν 32 ξεχωριστά καταστατικά, το καθένα με τους δικούς του αντίστοιχους κανονισμούς, που αφορούν την προστασία της ιδιωτικής ζωής σε εθνικό, επαρχιακό και σε ορισμένες περιπτώσεις δημοτικό επίπεδο. Επιπρόσθετα, οι περισσότερες περιοχές με εξαίρεση το Quebec και τη Nuvanut, έχουν θεσπίσει νομοθεσία που ασχολείται ειδικά με τον τομέα της υγείας και την προστασία των προσωπικών πληροφοριών για την υγεία. Σε ορισμένες επαρχίες, η υγειονομική νομοθεσία είναι ουσιαστικά παρόμοια με το Νόμο

Προστασίας Προσωπικών Πληροφοριών και Ηλεκτρονικών Εγγράφων (PIPEDA) και υπερισχύει του PIPEDA για δραστηριότητες σχετικές με την υγεία σε αυτές τις περιοχές.

Ο Καναδάς έχει δύο ομοσπονδιακούς νόμους περί απορρήτου που επιβάλλονται από το Γραφείο του Privacy Commissioner του Καναδά:

- ο **Νόμος περί απορρήτου Privacy Act**, ο οποίος καλύπτει τον τρόπο με τον οποίο η ομοσπονδιακή κυβέρνηση διαχειρίζεται τα προσωπικά στοιχεία
- ο **Νόμος περί Προστασίας Προσωπικών Πληροφοριών και Ηλεκτρονικών Εγγράφων (PIPEDA)**, ο οποίος καλύπτει τον τρόπο με τον οποίο οι επιχειρήσεις χειρίζονται τα προσωπικά στοιχεία.

Ο Νόμος περί απορρήτου (του 1985) σχετίζεται με το δικαίωμα ενός ατόμου να έχει πρόσβαση και να διορθώνει προσωπικές πληροφορίες που διατηρεί η κυβέρνηση του Καναδά σχετικά με το άτομο. Ο Νόμος ισχύει επίσης για τη συλλογή, χρήση και αποκάλυψη προσωπικών πληροφοριών από την Κυβέρνηση κατά την παροχή υπηρεσιών όπως συντάξεις, ασφάλιση εργασίας, ασφάλεια των συνόρων, ομοσπονδιακή αστυνόμευση και δημόσια ασφάλεια, είσπραξη φόρων. Ο Νόμος περί απορρήτου ισχύει μόνο για τα ιδρύματα της ομοσπονδιακής κυβέρνησης που αναφέρονται στη σχετική λίστα που συνοδεύει το νόμο. Ισχύει για όλες τις προσωπικές πληροφορίες που συλλέγει, χρησιμοποιεί και αποκαλύπτει η ομοσπονδιακή κυβέρνηση, περιλαμβάνοντας και προσωπικές πληροφορίες για ομοσπονδιακούς υπαλλήλους. (Laws Lois, 2020)

Ο Νόμος περί απορρήτου ορίζει τα παρακάτω προσωπικά στοιχεία ως καταγεγραμμένες πληροφορίες σχετικά με ένα αναγνωρίσιμο άτομο:

- φυλή, εθνικότητα, χρώμα, θρησκεία, ηλικία, οικογενειακή κατάσταση
- εκπαίδευση, ιατρικό, ποινικό ή εργασιακό ιστορικό, πληροφορίες σχετικά με χρηματοοικονομικές συναλλαγές
- οποιοδήποτε σύμβολο μπορεί να προσδιορίσει το άτομο
- διεύθυνση, δακτυλικά αποτυπώματα, τύπος αίματος
- προσωπικές απόψεις, εκτός εάν πρόκειται για άλλο άτομο
- ιδιωτική ή εμπιστευτική αλληλογραφία που αποστέλλεται σε κυβερνητικό ίδρυμα

- απόψεις ενός άλλου ατόμου για το εν λόγω άτομο
- το όνομα του ατόμου όταν εμφανίζεται με άλλες σχετικές προσωπικές πληροφορίες που επιτρέπουν την αποκάλυψή του σε άλλες περιπτώσεις ανωνυμοποίησης (Laws Lois, 2020)

Ο Νόμος περί Προστασίας Προσωπικών Πληροφοριών και Ηλεκτρονικών Εγγράφων (PIPEDA) είναι μια ομοσπονδιακή νομοθεσία που τέθηκε σε εφαρμογή το 2004. Ο σκοπός αυτού του νόμου είναι να ενθαρρύνει μια κουλτούρα στην οποία «η τεχνολογία διευκολύνει όλο και περισσότερο την κυκλοφορία και την ανταλλαγή πληροφοριών, με κανόνες που διέπουν τη συλλογή, χρήση και αποκάλυψη προσωπικών πληροφοριών με τρόπο που αναγνωρίζει το δικαίωμα της ιδιωτικότητας των ατόμων σε σχέση με τα προσωπικά τους στοιχεία και την ανάγκη των οργανισμών να συλλέγουν, να χρησιμοποιούν ή να αποκαλύπτουν προσωπικά στοιχεία για σκοπούς που ένα λογικό άτομο θα θεωρούσε κατάλληλο ανάλογα με τις περιστάσεις». Οι δέκα αρχές του PIPEDA είναι (Privacy Commisioner Canada, 2019):

- Ευθύνη: Ένας οργανισμός είναι υπεύθυνος για τις προσωπικές πληροφορίες που βρίσκονται υπό τον έλεγχό του και ορίζει ένα άτομο που είναι υπεύθυνο για τη συμμόρφωση του οργανισμού. Αυτός ο υπεύθυνος απορρήτου είναι αρμόδιος να μεριμνήσει για την κατανόηση και εφαρμογή των σχετικών κανόνων και να χειριστεί τα παράπονα.
- Προσδιορισμός σκοπιμότητας: Οι σκοποί για τους οποίους συλλέγονται οι πληροφορίες πρέπει να προσδιορίζονται πριν ή κατά τη στιγμή της συλλογής. Οι οργανισμοί πρέπει να συντάξουν αντίστοιχες εκθέσεις σκοπιμότητας.
- Συγκατάθεση: Η γνώση και συγκατάθεση του ατόμου απαιτούνται για τη συλλογή, χρήση ή αποκάλυψη προσωπικών πληροφοριών σε μια εμπορική δραστηριότητα. Η συγκατάθεση μπορεί να εκφραστεί ή να υπονοηθεί. Η Επιτροπή Απορρήτου συνιστά ρητή συγκατάθεση στις περισσότερες περιπτώσεις.
- Περιορισμός συλλογής: Οι πληροφορίες πρέπει να συλλέγονται για συγκεκριμένους σκοπούς και μπορούν να χρησιμοποιηθούν μόνο για αυτούς τους σκοπούς. Οι πληροφορίες δεν μπορούν να συλλεχθούν με παραπλάνηση ή εξαπάτηση των ατόμων σχετικά με τον σκοπό για τον οποίο προορίζονται.

- Περιορισμός χρήσης, αποκάλυψης και διατήρησης προσωπικών πληροφοριών: Οι οργανισμοί μπορούν να χρησιμοποιούν, να αποκαλύπτουν και να διατηρούν προσωπικά στοιχεία μόνο για τους συγκεκριμένους σκοπούς για τους οποίους συλλέχθηκαν και δεν πρέπει να τα διατηρήσουν περισσότερο από ό, τι απαιτείται για αυτούς τους συγκεκριμένους σκοπούς.
- Ακρίβεια: Οι προσωπικές πληροφορίες πρέπει να είναι ακριβείς, πλήρεις και ενημερωμένες.
- Διασφάλιση προστασίας: Ο οργανισμός πρέπει να προστατεύει τα προσωπικά στοιχεία από απώλεια ή κλοπή, καθώς και μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, αντιγραφή ή τροποποίηση. Το επίπεδο ασφάλειας πρέπει να είναι κατάλληλο σύμφωνα με την ευαισθησία των πληροφοριών. Τα άτομα με πρόσβαση πρέπει να υπογράφουν συμφωνίες εμπιστευτικότητας.
- Διαφάνεια: Οι πολιτικές απορρήτου ενός οργανισμού πρέπει να είναι άμεσα διαθέσιμες σε όλους.
- Ατομική πρόσβαση: Τα άτομα έχουν το δικαίωμα να γνωρίζουν ποιες προσωπικές πληροφορίες έχουν συλλεχθεί, πώς χρησιμοποιούνται, σε ποιον έχουν αποκαλυφθεί και έχουν τη δυνατότητα να αμφισβητήσουν την ακρίβεια και την πληρότητα των πληροφοριών και να διορθώσουν τυχόν λάθη.
- Συμμόρφωση: Τα άτομα πρέπει να τους επιτρέπεται να αντιμετωπίσουν τυχόν προκλήσεις σχετικά με τη συμμόρφωση του οργανισμού ως προς τις αρχές ιδιωτικότητας, προς τον επικεφαλής υπεύθυνο απορρήτου του οργανισμού.

2.5.2 Νομοθεσία για την υγεία

Κάθε επαρχία και επικράτεια έχουν τη δική τους νομοθεσία που ισχύει για τους φορείς της επαρχιακής κυβέρνησης υπερισχύοντας του Νόμου περί απορρήτου. Για τον ιδιωτικό τομέα, ορισμένες επαρχίες έχουν θεσπίσει νομοθεσία που είναι ουσιαστικά παρόμοια με την PIPEDA και επομένως προηγείται σε αυτές τις επαρχίες. Αυτή η νομοθεσία περιλαμβάνει τα παρακάτω (Colleaga, 2020):

- Alberta - Personal Information Protection Act
- British Columbia - Personal Information Protection Act

- Quebec - An Act Respecting the Protection of Personal Information in the Private Sector

Άλλες επαρχίες έχουν νομοθεσία περί προστασίας της ιδιωτικής ζωής στην υγειονομική περίθαλψη που είναι και πάλι είναι ουσιαστικά παρόμοια με την PIPEDA και επομένως υπερισχύει. Αυτή η νομοθεσία περιλαμβάνει τα παρακάτω (Colleaga, 2020):

- Ontario - Personal Health Information Protection Act
- New Brunswick - Personal Health Information Privacy and Access Act
- Newfoundland and Labrador - Personal Health Information Act

Τέλος, κάθε επαρχία και επικράτεια στον Καναδά έχει επίσης έναν Επίτροπο υπεύθυνο για την εποπτεία αυτής της νομοθεσίας.

Ο Νόμος περί Προστασίας Πληροφοριών για την Υγεία (PHIPA) είναι η ειδική νομοθεσία περί προστασίας της υγείας του Οντάριο, η οποία τέθηκε σε ισχύ την 1η Νοεμβρίου 2004. Το PHIPA διέπει τον τρόπο συλλογής, χρήσης και αποκάλυψης προσωπικών πληροφοριών για την υγεία. Ρυθμίζει τους επίτροπους πληροφοριών για την υγεία (custodians), καθώς και άτομα και οργανισμούς που λαμβάνουν προσωπικές πληροφορίες για την υγεία. Σχεδιάστηκε για να δώσει στα άτομα μεγαλύτερο έλεγχο του τρόπου συλλογής, χρήσης ή αποκάλυψης των προσωπικών τους πληροφοριών για την υγεία. Το PHIPA εξισορροπεί τα δικαιώματα απορρήτου των ατόμων με τη νόμιμη ανάγκη των οργανισμών να συλλέγουν, να χρησιμοποιούν και να αποκαλύπτουν προσωπικές πληροφορίες για την υγεία προκειμένου να παρέχουν αποτελεσματική και έγκαιρη υγειονομική περίθαλψη και να σχεδιάζουν και να διαχειρίζονται το δημόσιο χρηματοδοτούμενο σύστημα υγείας του Οντάριο. (Ontario Law, 2020)

Με κάποιες εξαιρέσεις, το PHIPA απαιτεί από τους καθορισμένους επίτροπους να λάβουν τη συγκατάθεσή πριν από τη συλλογή, τη χρήση ή την αποκάλυψη προσωπικών πληροφοριών υγείας. Επιπλέον, το PHIPA παρέχει στα άτομα το δικαίωμα πρόσβασης και αίτησης διόρθωσης των προσωπικών τους πληροφοριών υγείας. Το PHIPA παρέχει επίσης ένα τρόπο αποκατάστασης μέσω του Γραφείου του Επιτρόπου Πληροφοριών και Απορρήτου του Οντάριο (IPC) όταν έχουν παραβιαστεί τα δικαιώματα απορρήτου που

σχετίζονται με προσωπικές πληροφορίες υγείας. Το IPC είναι ο καθορισμένος φορέας εποπτείας, υπεύθυνος για τη διαχείριση και την επιβολή αυτών των κανόνων απορρήτου στον τομέα της υγείας. (IPC, 2015)

2.5.3 Εφαρμογή του απορρήτου στην υγεία

Το Καναδικό Ινστιτούτο για Πληροφορίες Υγείας (Canadian Institute for Health Information – CIHI) έχει δεσμευτεί να προστατεύει το απόρρητο των Καναδών και να διασφαλίζει την ασφάλεια των προσωπικών τους πληροφοριών για την υγεία. Είναι ένας οργανισμός συλλογής δεδομένων πληροφοριών για την υγεία. Δεδομένα που λαμβάνονται από νοσοκομεία και άλλες εγκαταστάσεις υγειονομικής περίθαλψης, κέντρα φροντίδας, περιφερειακές υγειονομικές αρχές, ιατρούς και κυβερνήσεις γνωστοποιούνται στο CIHI τηρώντας τη νομοθεσία περί απορρήτου και τη νομοθεσία σχετική με την υγεία και υπόκειται σε σχετικές συμφωνίες ανταλλαγής δεδομένων. (CIHI, 2020)

Το CIHI χρησιμοποιεί πληροφορίες για την υγεία για τη διενέργεια αναλύσεων σχετικά με τα συστήματα υγείας του Καναδά και την υγεία των Καναδών κατά τρόπο συνεπή με το σκοπό του καταστατικού του και τις βασικές λειτουργίες του, ειδικά για την παροχή πληροφοριών που επιτρέπουν τη βελτίωση της υγειονομικής περίθαλψης, της απόδοσης του συστήματος υγείας και της υγείας του πληθυσμού σε όλα τα επίπεδα. Γενικά, το CIHI χρησιμοποιεί μη αναγνωρίσιμα δεδομένα για σκοπούς αναλυτικής Big Data. Τα σύνολα δεδομένων που χρησιμοποιούνται για την αναλυτική που πραγματοποιείται στο CIHI δεν περιέχουν ονόματα ή απευθείας αναγνωριστικά, όπως αριθμούς υγειονομικής περίθαλψης, ημερομηνίες γέννησης και ταχυδρομικούς κώδικες. (CIHI, 2020)

Οι κοινοποιήσεις πληροφοριών για την υγεία του CIHI γίνονται στον υψηλότερο δυνατό βαθμό ανωνυμίας, αλλά διατηρώντας τους ερευνητικούς και αναλυτικούς σκοπούς για τους οποίους συλλέχθηκαν. Το CIHI δημοσιοποιεί συγκεντρωτικά δεδομένα με τρόπο που έχει σχεδιαστεί για να ελαχιστοποιεί κάθε κίνδυνο επαναπροσδιορισμού των ατόμων στα οποία ανήκουν. Γενικά, τα δεδομένα που αποκαλύπτονται σε τρίτους

για ερευνητικούς σκοπούς έχουν τη μορφή απο-προσδιορισμένων δεδομένων σε επίπεδο εγγραφής ή συγκεντρωτικών δεδομένων. Όσοι οργανισμοί αιτούνται την απόκτηση προσωπικών δεδομένων υποχρεούνται να συνάψουν συμφωνία μη αποκάλυψης / εμπιστευτικότητας με το CIHI. Η συμφωνία θεσπίζει στοιχεία ελέγχου απορρήτου και ασφάλειας που πρέπει να τηρούνται από τον οργανισμό παραλήπτη. (CIHI, 2020)

Το CIHI δεν αποκαλύπτει προσωπικές πληροφορίες για την υγεία, εκτός από τις ακόλουθες περιστάσεις και όταν οι παραλήπτες έχουν συνάψει συμφωνία προστασίας δεδομένων ή άλλα νομικά δεσμευτικά έγγραφα με το CIHI (CIHI, 2020):

- Ο παραλήπτης έχει λάβει τη συγκατάθεση των ενδιαφερομένων ατόμων.
- Ο παραλήπτης είναι μια καθορισμένη οντότητα σύμφωνα με το νόμο PHIPA του Οντάριο με σκοπό τη διευκόλυνση ή τη βελτίωση της παροχής υγειονομικής περίθαλψης, υπό τον όρο ότι πληρούνται οι απαιτήσεις του PHIPA και του CIHI.
- Η αποκάλυψη απαιτείται από το νόμο.

2.6 Ιαπωνία

2.6.1 Νομοθεσία για προσωπικά δεδομένα

Οι ακόλουθοι νόμοι και κανονισμοί αποτελούν τη βασική νομοθεσία στην Ιαπωνία για την προστασία των Προσωπικών Πληροφοριών από το 2005:

- Νόμος για την προστασία των προσωπικών πληροφοριών (Act on the Protection of Personal Information - APPI), νόμος αριθ. 57 του 2003
- Νόμος για την προστασία των προσωπικών πληροφοριών που κατέχουν τα διοικητικά όργανα (Act on the Protection of Personal Information Held by Administrative Organs), νόμος αριθ. 95 του 1988, τροποποιήθηκε το 2003
- Νόμος για την προστασία των προσωπικών πληροφοριών που κατέχουν ανεξάρτητοι διοικητικοί φορείς (Act on the Protection of Personal Information Held by Independent Administrative Agencies)
- Τοπικοί κανονισμοί (jyourei) που νομοθετούνται από τις τοπικές κυβερνήσεις.

Η Επιτροπή Προστασίας Προσωπικών Πληροφοριών (PPC) η οποία είναι ο κύριος οργανισμός που εποπτεύει την εφαρμογή και εφαρμογή του APPI, εκδίδει γενικές οδηγίες για την εφαρμογή του APPI. Υπάρχουν επίσης άλλες οδηγίες για συγκεκριμένους τομείς που εκδίδονται από τα αρμόδια υπουργεία. (ICLG, 2020)

Νόμος για την προστασία των προσωπικών πληροφοριών APPI

Το APPI είναι η κύρια νομοθεσία για την προστασία των δεδομένων στην Ιαπωνία. Βασική αρχή της APPI είναι η σωστή διαχείριση των προσωπικών πληροφοριών, όπως ορίζεται στο Άρθρο 2, παράγραφος 1, σύμφωνα με την αρχή του σεβασμού του ατόμου. Τα Κεφάλαια 2 και 3 καθορίζουν το βασικό πλαίσιο των αρμοδιοτήτων της εθνικής και των τοπικών κυβερνήσεων για την προστασία των προσωπικών πληροφοριών. Σύμφωνα με το άρθρο 7 του APPI, το Συμβούλιο έχει καθιερώσει τη «Βασική Πολιτική για την Προστασία των Προσωπικών Πληροφοριών» (Kojin Jyouhou no Hogo ni kansuru Kihon Houshin).

Το Κεφάλαιο 4 ρυθμίζει τη χρήση των προσωπικών πληροφοριών από ιδιωτικές επιχειρήσεις και καθορίζει τις υποχρεώσεις των επιχειρήσεων που χειρίζονται προσωπικά στοιχεία (Kojin Joho Toriatsukai Jigyosha)» («Χειριστές δεδομένων»), όπως ορίζονται στο άρθρο 2, παράγραφος 5 του APPI. Οποιοσδήποτε υπεύθυνος επιχείρησης που χρησιμοποιεί μια βάση δεδομένων προσωπικών πληροφοριών θεωρείται χειριστής ανεξάρτητα από την κλίμακα της βάσης δεδομένων προσωπικών πληροφοριών (η εξαίρεση που δινόταν σε μικρές επιχειρήσεις με βάση δεδομένων προσωπικών πληροφοριών λιγότερων από 5.000 ατόμων καταργήθηκε το 2017). Ο χειρισμός δεδομένων από διοικητικά όργανα και ανεξάρτητους διοικητικούς οργανισμούς ρυθμίζεται σύμφωνα με τους νόμους που αναφέρθηκαν στην εισαγωγική παράγραφο για τη νομοθεσία στην Ιαπωνία. Τέλος, ενα νομοσχέδιο για την περαιτέρω τροποποίηση του APPI υποβλήθηκε στις 10 Μαρτίου 2020. (PPC, 2020)

Μια επιχείρηση μπορεί να χρησιμοποιήσει ένα λογότυπο που ονομάζεται «Σήμα Απορρήτου» που δείχνει τη συμμόρφωσή του με τους σχετικούς νόμους και τα βιομηχανικά πρότυπα της Ιαπωνίας (JIS Q 15001: 2006 [Σύστημα διαχείρισης

προστασίας προσωπικών πληροφοριών]) που καθιερώθηκε από το Κέντρο Ανάπτυξης Πληροφορικής της Ιαπωνίας. Το JIS Q 15001 δεν είναι νόμος, αλλά, σε ορισμένες περιπτώσεις, παρέχει υψηλότερο επίπεδο προτύπων από το APPI. (IHS, 2017)

Η Επιτροπή Προστασίας Προσωπικών Πληροφοριών (PPC), ως ανεξάρτητος ρυθμιστικός φορέας, εξουσιοδοτείται να συμβουλεύει έναν Χειριστή Δεδομένων ή να απαιτεί την υποβολή έκθεσης σχετικά με το χειρισμό προσωπικών πληροφοριών στο βαθμό που είναι απαραίτητο για την εφαρμογή του APPI (APPI, άρθρα 40 και 41). Εάν ένας χειριστής παραβιάσει το APPI, η PPC μπορεί να εμπλακεί και να αποτρέψει τη συνέχιση της παράβασης και να λάβει άλλα απαραίτητα μέτρα για την αντιμετώπιση των συνεπειών της παράβασης (άρθρο 42 παρ 1.). Εάν η PPC το κρίνει απαραίτητο και πληρούνται ορισμένες προϋποθέσεις, μπορεί να διατάξει τον Διαχειριστή να λάβει τα προτεινόμενα μέτρα ή να σταματήσει την παράβαση και να λάβει άλλα απαραίτητα μέτρα για να διορθώσει τις συνέπειες (άρθρο 42 παρ. 2 και 3). (PPC, 2020)

Ο Νόμος APPI (η πιο πρόσφατη έκδοσή του 2016) στην Ιαπωνία επιδιώκει να προστατεύσει την ιδιωτικότητα των δεδομένων σε παρόμοια επίπεδα με την αντίστοιχη νομοθεσία της Ευρωπαϊκής Ένωσης (GDPR) αλλά, οι επικριτές αναφέρουν ότι για την ώρα δεν πληροί τις υψηλές απαιτήσεις του κανονισμού της ΕΕ. Μια βασική διαφορά είναι ότι οι ανώνυμες πληροφορίες νοούνται ως μη προσωπικές πληροφορίες στην εφαρμογή του APPI στην Ιαπωνία, ενώ ενδέχεται να αποτελούν προσωπικές πληροφορίες βάσει της οδηγίας για τα δεδομένα της ΕΕ. (Tsuji, 2017)

2.6.2 Νομοθεσία για ιδιωτικότητα στην Υγεία

Η βασική νομοθεσία που εφαρμόζεται στις επιχειρήσεις υγειονομικής περίθαλψης είναι ο Νόμος για την Εξασφάλιση Ποιότητας, Αποτελεσματικότητας και Ασφάλειας των Προϊόντων, συμπεριλαμβανομένων των φαρμακευτικών προϊόντων και των ιατρικών συσκευών. Εάν το προϊόν εμπίπτει στην κατηγορία «ιατροτεχνολογικό προϊόν» όπως ορίζεται στον Νόμο, είναι απαραίτητο να ληφθεί έγκριση του προϊόντος και άδεια για κατασκευή και πώληση. Ο όρος «ιατρική συσκευή» ορίζεται ως «συσκευές ή όργανα κ.λπ. που προορίζονται για χρήση στη διάγνωση, θεραπεία ή πρόληψη ασθενειών σε

ανθρώπους ή ζώα, ή προορίζονται να επηρεάσουν τη δομή ή τη λειτουργία των σωμάτων ανθρώπων ή ζώων». Τα ιατροτεχνολογικά προϊόντα ταξινομούνται σε τέσσερις κατηγορίες, ανάλογα με τους κινδύνους για τον άνθρωπο ή τα ζώα. Οι εγκρίσεις και οι άδειες διαφέρουν επίσης ανάλογα με κάθε κατηγορία. Απαγορεύεται η διαφήμιση ιατρικών συσκευών που περιέχουν παραπλανητικές πληροφορίες. Εάν ένα ιατροτεχνολογικό προϊόν δεν λάβει έγκριση ως συσκευή, απαγορεύεται αυστηρά η διαφήμιση που περιέχει ιατρικές υπηρεσίες. (Matsuo, 2009)

Επιπλέον, ενδέχεται να εφαρμόζονται οι ακόλουθοι διάφοροι κανονισμοί, ανάλογα με τον τύπο της επιχείρησης: (ICLG, 2020)

- Νόμος Ιατρικής Πρακτικής (τηλεδιάγνωση, έλεγχος γονιδίων κ.λπ.)
- Νόμος Φροντίδας Υγείας (ίδρυση εταιρείας υγειονομικής περίθαλψης)
- Νόμος Φαρμάκων (συνταγή απομακρυσμένης ιατρικής)
- Νόμος για τη χρήση της τεχνολογίας τηλεπικοινωνιών στη συντήρηση εγγράφων, που διεξάγεται από ιδιωτικούς επιχειρηματίες (ηλεκτρονικό ιατρικό αρχείο)
- Νόμος για την Αναγεννητική Ιατρική
- Νόμος για Κλινικές δοκιμές
- Ασφαλιστικοί νόμοι
- Νόμος περί ευθύνης προϊόντος

Ποιοι οργανισμοί είναι υπεύθυνοι; Το Υπουργείο Υγείας, Εργασίας και Πρόνοιας είναι υπεύθυνο για τον έλεγχο στα ιατροτεχνολογικά προϊόντα (που προορίζονται για ανθρώπους). Το Υπουργείο αναθέτει στον Οργανισμό Φαρμακευτικών και Ιατρικών Συσκευών (PMDA) να διεξάγει έρευνες για εγκρίσεις. Η άδεια για την κατασκευή και τη διεξαγωγή της πώλησης ενός ιατροτεχνολογικού προϊόντος πρέπει να γίνει μέσω του νομαρχιακού κυβερνήτη της περιοχής. Ο APPI εμπίπτει στη δικαιοδοσία της Επιτροπής Προστασίας Προσωπικών Πληροφοριών και ο Οργανισμός Καταναλωτικών Υποθέσεων έχει δικαιοδοσία επί του Νόμου περί Εμπορικών Συναλλαγών, και του Νόμου περί Καταναλωτικών Συμβάσεων. (PMDA, 2020)

2.6.3 Ιδιωτικότητα και Big Data στην υγεία

Ένας πάροχος ψηφιακής πλατφόρμας με υπηρεσίες υγείας είναι πολύ πιθανό να χρειάζεται να λαμβάνει προσωπικές και ευαίσθητες πληροφορίες στις περισσότερες περιπτώσεις. Άρα θα πρέπει να δώσει Ιδιαίτερη προσοχή στον νόμο για την προστασία των προσωπικών πληροφοριών (APPI). Ο Νόμος για τα ανώνυμα ιατρικά δεδομένα που συμβάλλουν στην έρευνα και ανάπτυξη στην ιατρική, θεσπίστηκε το 2017 και αναμένεται θα διευκολύνει τη χρήση Big Data στην υγεία. Με άλλα λόγια, κατέστη δυνατό για τα ιατρικά ιδρύματα να παρέχουν σε εξουσιοδοτημένους χειριστές ιατρικές πληροφορίες των ασθενών και οι εξουσιοδοτημένοι χειριστές να μπορούν να δημιουργήσουν ανωνυμοποιημένες πληροφορίες και να παρέχουν τις πληροφορίες αυτές σε όσους ενδιαφέρονται. (Japanese Agancy, 2019)

Το 2013, η Ιαπωνική κυβέρνηση ανακοίνωσε ότι τη δημιουργία ενός κεντρικού σχεδίου για την ιατρική περίθαλψη με σκοπό τη βελτιστοποίηση της ιατρικής θεραπείας στο μέλλον (Υπουργείο Υγείας, Εργασίας και Πρόνοιας). Η κυβέρνηση πρότεινε ένα μοντέλο ιατρικής θεραπείας που θα εκμεταλλευόταν την τεχνολογία της πληροφορίας, προτείνοντας «πληροφοριοποίηση» ως λύση στα προβλήματα υγείας που θέτει η γερασμένη κοινωνία της Ιαπωνίας. Η κοινή χρήση Big Data για ιατρικές παθήσεις μπορεί να χρησιμοποιηθεί για την ανάλυση ασθενειών όπως ο διαβήτης και άλλες συνοδευτικές ασθένειες. Οι εγκαταστάσεις μακροχρόνιας περίθαλψης και ιατρικών επεμβάσεων μπορούν να τοποθετηθούν σε διαφορετικές τοποθεσίες στην Ιαπωνία βάσει αυτών των δεδομένων και οι ασθενείς μπορούν να ενθαρρυνθούν να ελέγχουν την υγεία τους περισσότερο από το σπίτι, καθώς ο αριθμός των νοσοκομειακών κρεβατιών είναι περιορισμένος στην Ιαπωνία. Από την άλλη, το σύστημα μπορεί να αναγνωρίσει τους ασθενείς που όντως χρειάζονται μακροχρόνια περίθαλψη και να τους διανείμει στο κατάλληλο νοσοκομείο. Αυτή η κοινή χρήση δεδομένων τέλος βοηθάει και στην προληπτική θεραπεία. Οι παραπάνω χρήσεις των Big Data στην υγεία ενθαρρύνθηκαν στο προαναφερθέν σχέδιο του Υπουργείου.

Η ιαπωνική κυβέρνηση, στην πραγματικότητα, πρότεινε μια προληπτική προσέγγιση για την υγεία με σκοπό τη μείωση των αυξανόμενων ιατρικών εξόδων που προκαλούνται από ασθένειες που οφείλονται στο σύγχρονο τρόπο ζωής που συχνά οδηγούν σε άλλες σοβαρές καταστάσεις. Οι ασθενείς είναι πλέον σε θέση να

αποθηκεύουν τα δικά τους ιατρικά δεδομένα στο διαδίκτυο, ενώ μπορούν να επιλέξουν ιατρικές και υγειονομικές υπηρεσίες κοινοποιώντας τους τα δεδομένα υγείας τους. (Tsuji, 2017)

Ενότητα 2: Ερευνητική Προσέγγιση

3.1 Γενικά στοιχεία της έρευνας

Σκοπός μελέτης

Σκοπός της παρούσας εργασίας είναι η διερεύνηση των στάσεων των συμμετεχόντων σε σχέση με τα ηλεκτρονικά δεδομένα στο χώρο της υγείας και την ασφάλειά τους. Επίσης, η μελέτη του μεγέθους της επιρροής των κοινωνικο-δημογραφικών παραγόντων στις προαναφερθείσες παραμέτρους.

Πληθυσμός στόχος

Νυν και πρώην εργαζόμενοι (με υγειονομικές ή διοικητικές ειδικότητες) σε χώρους υγείας σε διάφορες χώρες.

Πληθυσμός πρόσβασης

Νυν και πρώην εργαζόμενοι σε χώρους υγείας (με υγειονομικές ή διοικητικές ειδικότητες) στην Ελλάδα, στον Καναδά και στη Γερμανία.

Κριτήρια ένταξης και αποκλεισμού στη μελέτη

Κριτήρια ένταξης.

- Ηλικία 20 ετών και άνω.
- Ικανότητα επικοινωνίας και γνώση της ελληνικής ή της αγγλικής γλώσσας.
- Θέληση συμμετοχής στη μελέτη

Κριτήρια αποκλεισμού

- Ηλικία κάτω των 20 ετών.
- Δυσκολία κατανόησης της ελληνικής ή της αγγλικής γλώσσας.
- Άρνηση συμμετοχής στη μελέτη.

3.2 Μεθοδολογία

Η έρευνα πραγματοποιήθηκε στη Θεσσαλονίκη μεταξύ 4 Αυγούστου και 8 Σεπτεμβρίου 2020 στα πλαίσια του Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών "Δίκαιο και Πληροφορική" του Πανεπιστημίου Μακεδονίας. Η μελέτη πραγματοποιήθηκε με αυτοσυμπληρούμενα ερωτηματολόγια. Το ερωτηματολόγιο μοιράστηκε ηλεκτρονικά στους συμμετέχοντες μέσω της ηλεκτρονικής πλατφόρμας Google Forms. Οι συμμετέχοντες ενημερώθηκαν για τους σκοπούς της συμπλήρωσης των ερωτηματολογίων και τη διασφάλιση της ανωνυμίας. Η συμμετοχή των ατόμων ήταν εθελοντική και η συλλογή των ερωτηματολογίων έγινε από την ερευνήτρια. Οι συμμετέχοντες ήταν από την Ελλάδα, τον Καναδά και τη Γερμανία, ενώ το ερωτηματολόγιο χωριζόταν σε 2 μέρη :

1) Το πρώτο μέρος του ερωτηματολογίου σχετιζόταν με τα κοινωνικά-δημογραφικά στοιχεία των συμμετεχόντων (φύλο, ηλικία, επάγγελμα, οικογενειακή κατάσταση/ αριθμός παιδιών, τύπος εργασιακού πλαισίου, τόπος κατοικίας, χρόνια επαγγελματικής εμπειρίες).

2) Το δεύτερο μέρος περιείχε 14 ερωτήσεις που σχετίζονταν με την ασφάλεια των ηλεκτρονικών δεδομένων στο χώρο της υγείας.

Επειδή μας ενδιέφεραν οι άνθρωποι που εργάζονται στους χώρους της υγείας ο βασικός πληθυσμός στόχος ήταν οι διάφορες υγειονομικές ειδικότητες καθώς και το διοικητικό προσωπικό που εργάζεται στους χώρους αυτούς και όχι οι εργαζόμενοι στο χώρο της πληροφορικής γενικά. Για αυτό το λόγο στο ειδικό μέρος του ερωτηματολογίου υπάρχουν λίγες τεχνικές ερωτήσεις.

3.2.1. Δειγματοληπτική μέθοδος

Ως καταλληλότερη μέθοδος, για την συλλογή των δεδομένων της παρούσας μελέτης, κρίθηκε η δειγματοληψία «ευκολίας», καθώς όπως προαναφέρθηκε προϋπόθεση για τη συμμετοχή σε αυτή είναι η επιθυμία του ατόμου. Η ερευνητική χρησιμότητα και η αντιπροσωπευτικότητα ενός τέτοιου δείγματος είναι αμφισβητήσιμη για την εξαγωγή συμπερασμάτων που να ισχύουν στο γενικό πληθυσμό. Παρόλα αυτά η συγκεκριμένη

τεχνική δειγματοληψίας είναι πολύ διαδομένη όταν δεν δύναται να υπάρχει άμεση πρόσβαση σε ολόκληρο των πληθυσμό που μας αφορά (ανθρώπους που δούλεψαν/ δουλεύουν στο χώρο της υγείας είτε με υγειονομικές ειδικότητες είτε με διοικητικές ειδικότητες).Με αυτήν την τεχνική δειγματοληψίας θεωρείται ότι τα αποτελέσματα της έρευνας μπορούν να γενικευθούν σε πληθυσμούς που έχουν χαρακτηριστικά παρόμοια με αυτά το δείγματος.

3.2.2 Στατιστική ανάλυση

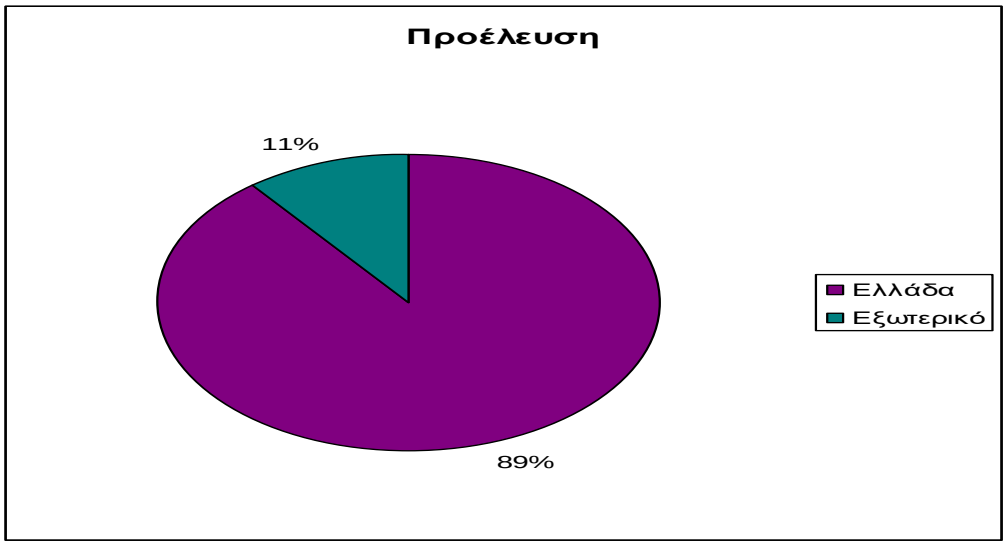
Για την περιγραφική στατιστική ανάλυση, οι διακριτές μεταβλητές εκφράστηκαν με τη «συχνότητα». Για τη μελέτη της σχέσης μεταξύ μιας αριθμητικής και μίας κατηγορικής μεταβλητής έγινε χρήση του ελέγχου των Kruskal-Wallis, γιατί δεν τηρούνταν η προϋπόθεση της κανονικότητας της κατανομής. Για τη μελέτη της σχέσης μεταξύ δυο κατηγορικών μεταβλητών έγινε χρήση του ελέγχου χ^2. Για τη μελέτη των συσχετίσεων μεταξύ 2 μεταβλητών χρησιμοποιήθηκε ο συντελεστής συσχέτισης του Pearson (r). Για την στατιστική επεξεργασία των δεδομένων έγινε χρήση του λογισμικού SPSS 20. Η ελάχιστη τιμή του επιπέδου στατιστικής σημαντικότητας, p-value, ορίζεται στο 5%. Ως υποδιαστολή χρησιμοποιείται η τελεία.

3.3 Αποτελέσματα

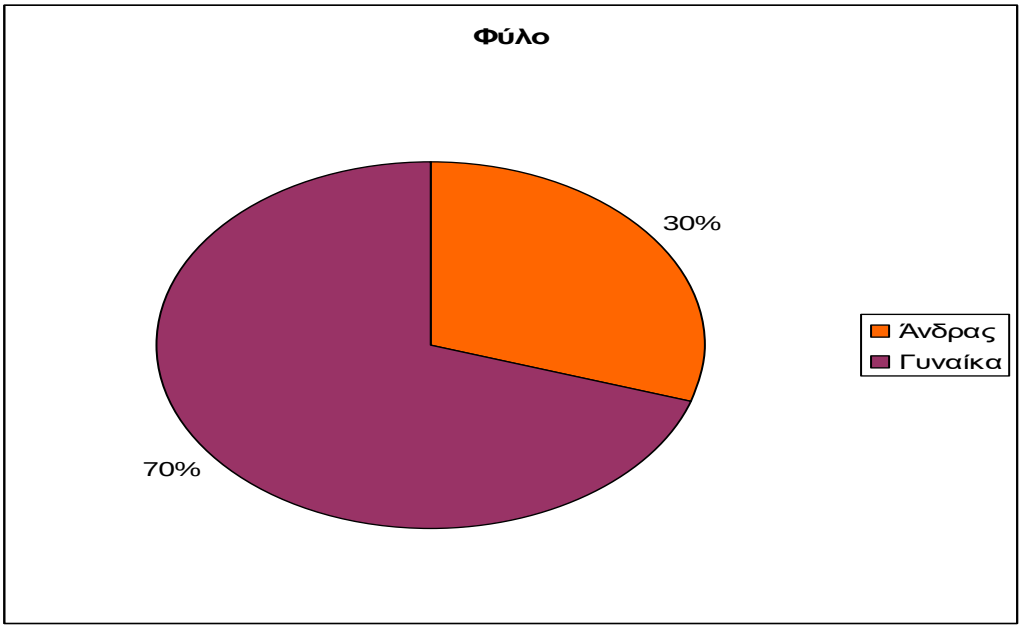
3.3.1 Περιγραφική στατιστική

3.3.1.α. Δημογραφικά στοιχεία

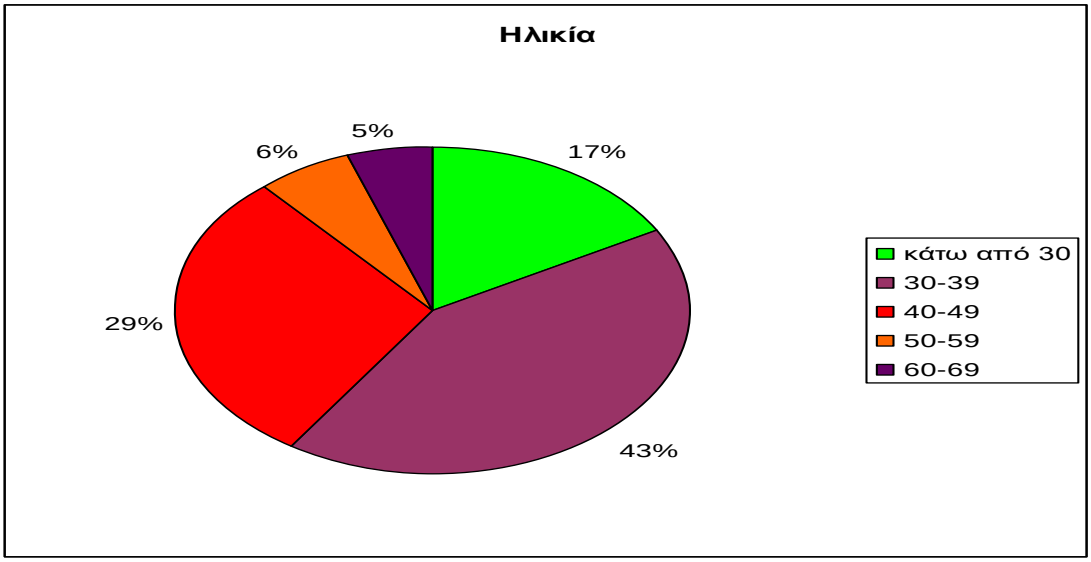
Το δείγμα της μελέτης αποτελείται από 113 άτομα (79 γυναίκες και 34 άνδρες). Σε σχέση με τη χώρα η μεγάλη πλειοψηφία των συμμετεχόντων ήταν από την Ελλάδα. Περίπου 9 στους 10 συμμετέχοντες ήταν από την Ελλάδα. Αυτό ήταν αναμενόμενο δεδομένου ότι η ερευνητική ομάδα και το εκπαιδευτικό ίδρυμα για το οποίο δεξιέγεται η έρευνα ήταν από την Ελλάδα. Από τους συμμετέχοντες του εξωτερικού οι 8 ήταν από τον Καναδά και οι 4 από τη Γερμανία.



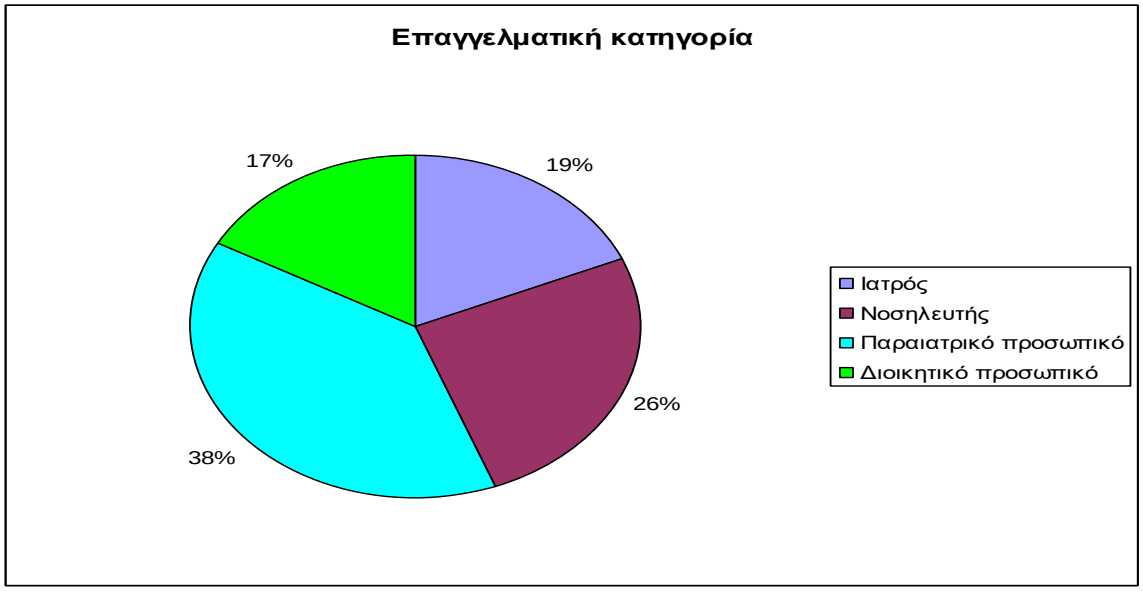
Στο δείγμα μας οι γυναίκες ήταν σαφώς περισσότερες από τους άντρες. Περίπου τα 7/10 των συμμετεχόντων του δείγματος ήταν γυναίκες. Φαίνεται ότι στο τρέχον δείγμα ότι ο χώρος της υγείας έχει σαφή ισχυρή εκπροσώπηση των γυναικών.



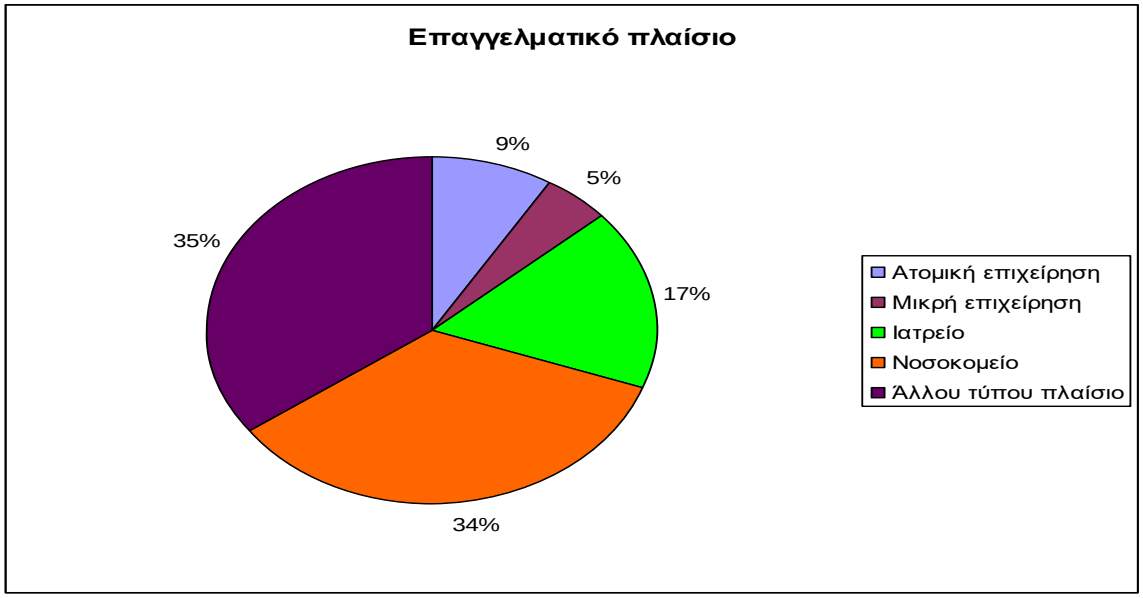
Σε σχέση με την ηλικία των συμμετεχόντων το σημαντικό κομμάτι των συμμετεχόντων ανήκει στη δεύτερη και στην τρίτη ηλικιακή κατηγορία, είναι δηλαδή από 30 μέχρι 49 ετών. Είναι λογικό η ομάδα αυτή να εμπλέκεται περισσότερα με τα επαγγελματικά καθώς οι περισσότεροι άνθρωποι δεν έχουν συνταξιοδοτηθεί σε αυτές τις ηλικίες ενώ έχουν τελειώσει από τις υποχρεώσεις που τους εμποδίζουν στην αναζήτηση εξειδικευμένης εργασίας (για παράδειγμα σπουδές, στρατιωτική θητεία).



Το σημαντικότερο κομμάτι των συμμετεχόντων, περίπου τα 2/5 του δείγματος, ανήκει στο παραϊατρικό προσωπικό. Αυτό συμβαίνει ενδεχομένως γιατί οι ειδικότητες που ανήκουν στο χώρο της υγείας εκτός των ιατρών και νοσηλευτών είναι αρκετές [για παράδειγμα ψυχολόγοι, εργοθεραπευτές, λογοθεραπευτές, φυσικοθεραπευτές].

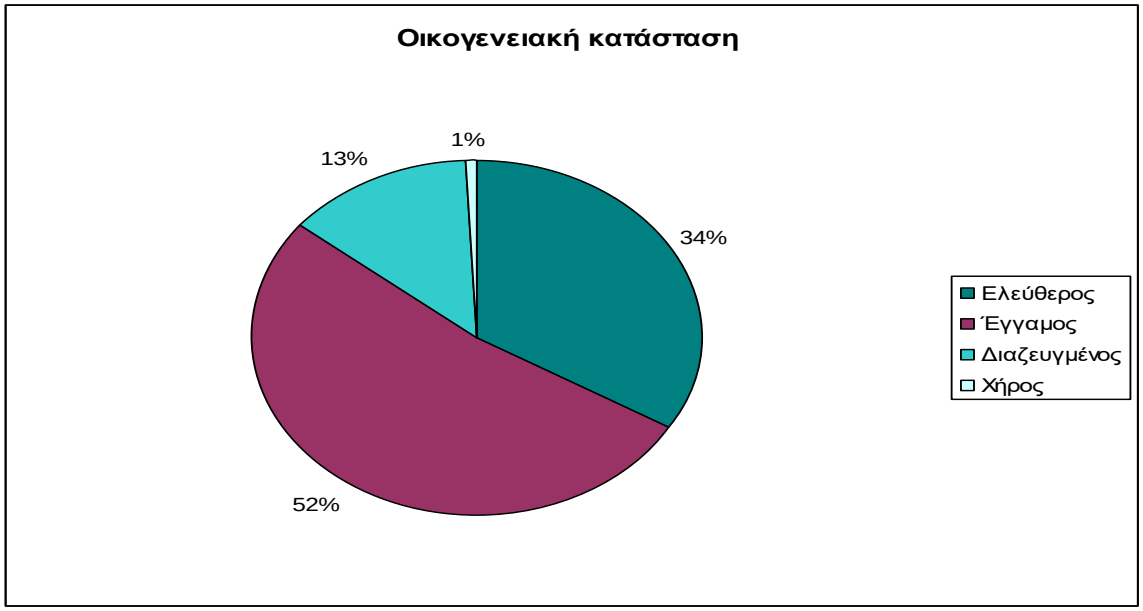


Σε σχέση με τον τύπο του εργασιακού πλαισίου τα 2/3 δουλεύουν είτε σε άλλου τύπου εργασιακό πλαίσιο, είτε σε νοσοκομείο. Οι συμμετέχοντες που εργάζονται σε μικρές επιχειρήσεις (όπως είναι τα θεραπευτήρια) είναι μόλις στο 5% των συμμετεχόντων.

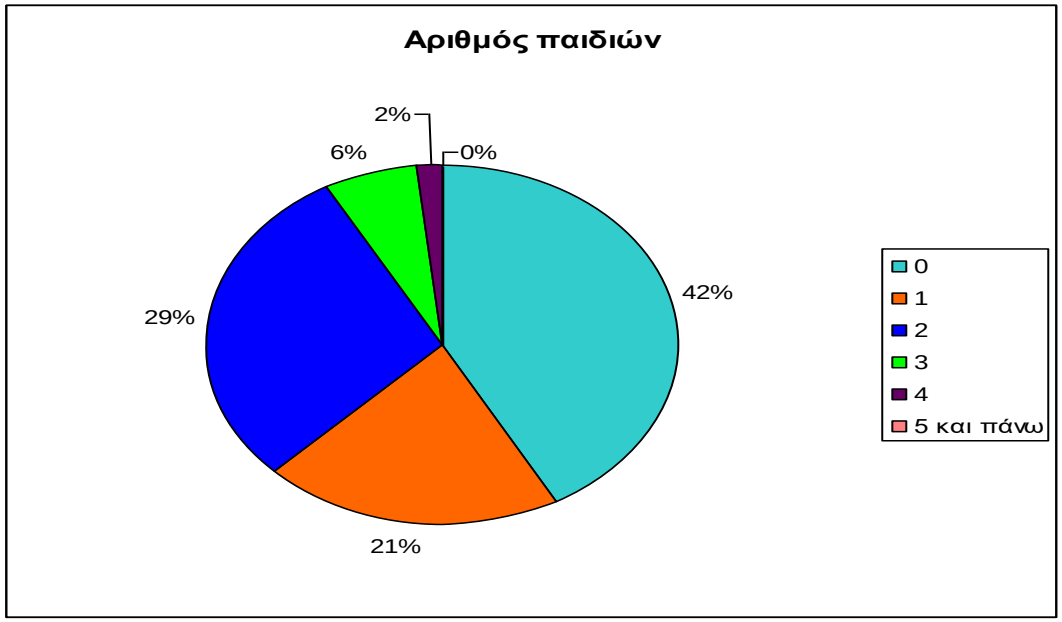


Σε σχέση με το εκπαιδευτικό επίπεδο των συμμετεχόντων φαίνεται ότι περίπου οι μισοί συμμετέχοντες είναι απόφοιτοι τριτοβάθμιας εκπαίδευσης (Ανώτατο Εκπαιδευτικό Ίδρυμα ή Ανώτατο Τεχνολογικό Εκπαιδευτικό Ίδρυμα), ενώ το 1/3 των συμμετεχόντων είναι κάτοχοι μεταπτυχιακού τίτλου.

Σε σχέση με την οικογενειακή κατάσταση των συμμετεχόντων περίπου οι μισοί εκ ων συμμετεχόντων είναι έγγαμοι, ενώ το 1/3 είναι ελεύθεροι..

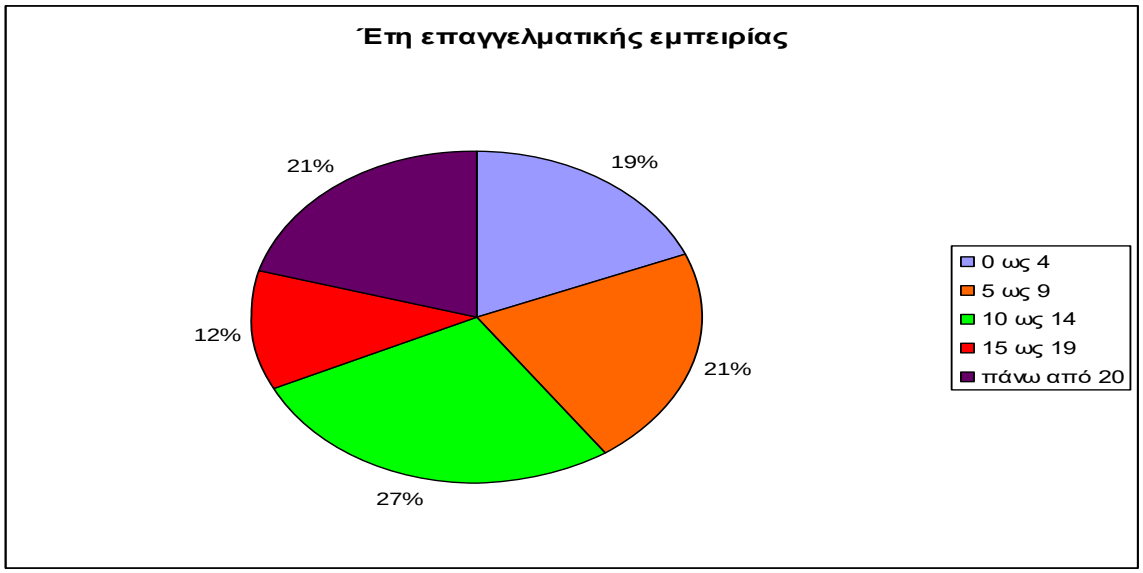


Σε σχέση με τον αριθμό των παιδιών περίπου τα 2/5 του δείγματος δεν έχουν κάποιο παιδί, ενώ από το σύνολο των συμμετεχόντων οι μισοί έχουν 1 ή 2 παιδιά.



Σε σχέση με τον τόπο κατοικίας σχεδόν οι μισοί κατάγονται από τη Θεσσαλονίκη. Αυτό είναι αναμενόμενη μιας και η ερευνήτρια αλλά και το ερευνητικό ίδρυμα στο πλαίσιο του οποίο εκπονείται η παρούσα έρευνα είναι στην περιοχή της Θεσσαλονίκης.

Σε σχέση με τα έτη επαγγελματικής εμπειρίας οι περισσότεροι συμμετέχοντες έχουν επαγγελματική εμπειρία μεταξύ 10 και 14 ετών, αλλά φαίνεται ότι σε αυτήν τη δημογραφική κατηγορία οι συμμετέχοντες είναι μοιρασμένοι.

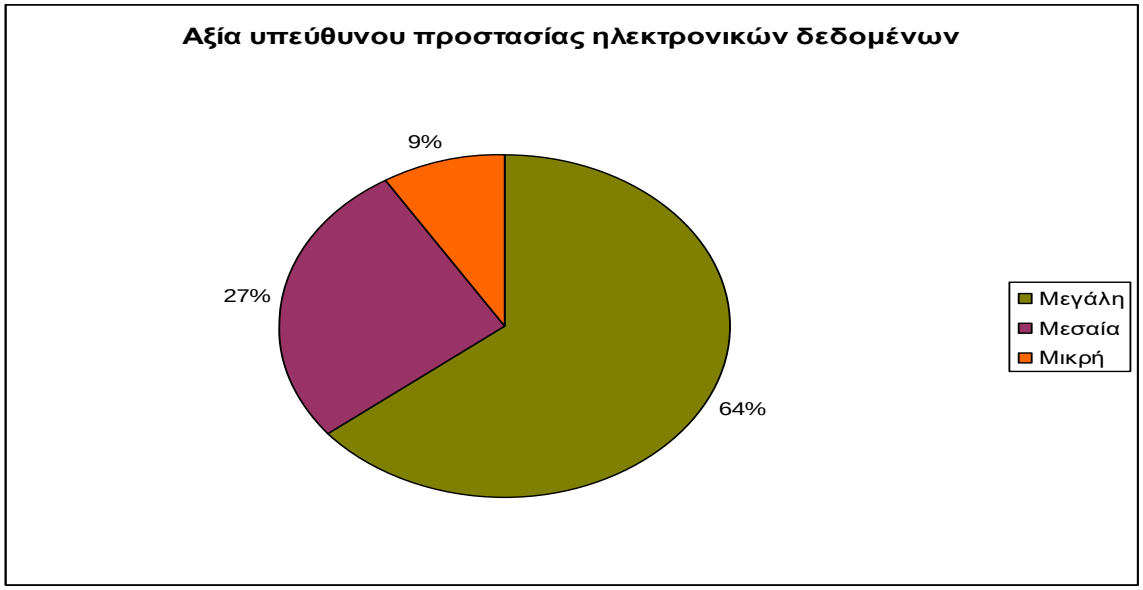


3.3.1.β. Ειδικές ερωτήσεις

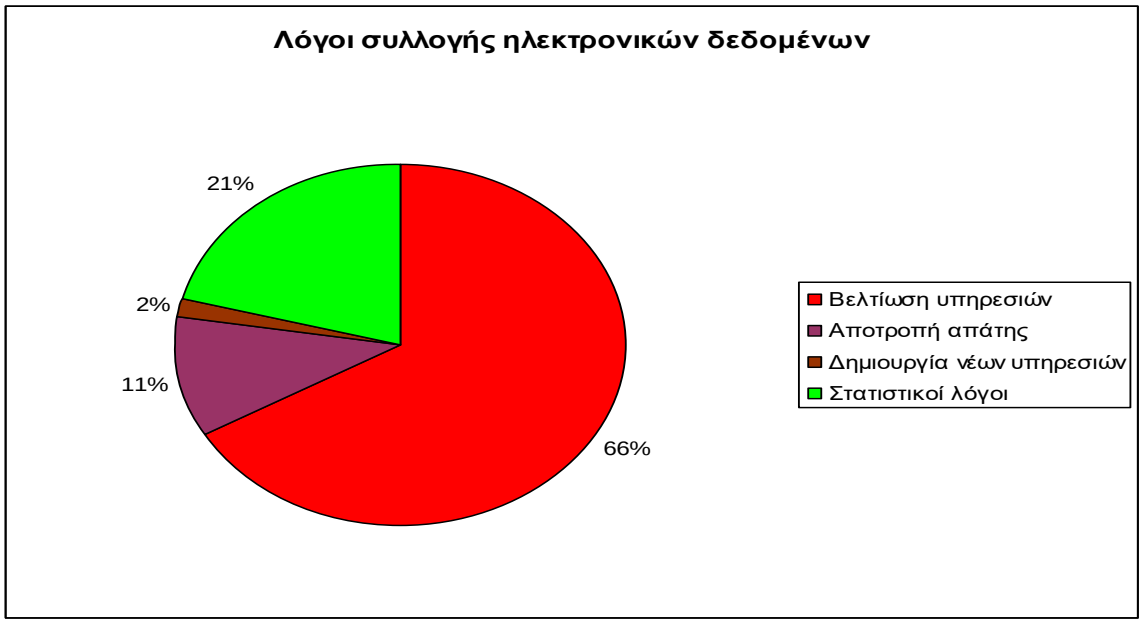
Στην ερώτηση τι είδους δεδομένα μαζεύονται από τη δομή υγείας στην οποία εργάζονται, τα 3/5 των συμμετεχόντων ανέφεραν ότι μαζεύουν δομημένα ηλεκτρονικά δεδομένα όπως οι ηλεκτρονικοί φάκελοι των ασθενών, ενώ στους υπόλοιπους συμμετέχοντες είναι οι μοιρασμένες οι απαντήσεις μεταξύ αδόμητων και ημι-δομημένων δεδομένων.

Στην ερώτηση αν υπάρχει κάποιος υπεύθυνος προστασίας ηλεκτρονικών δεδομένων σχεδόν οι μισοί απάντησαν ότι δεν έχουν στο εργασιακό τους πλαίσιο κάποιον υπεύθυνο προστασίας ηλεκτρονικών δεδομένων. Αυτό δεν αποτελεί έκπληξη δεδομένου ότι οι μισοί περίπου συμμετέχοντες της έρευνας δήλωσαν ότι δουλεύουν σε ατομικές ή σε μικρές επιχειρήσεις που είναι συνηθισμένες στο χώρο της υγείας (για παράδειγμα ιατρεία, θεραπευτήρια, αγροτικά ιατρεία). Από ότι φαίνεται στο εξωτερικό είναι συνηθέστερη η ύπαρξη ενός υπεύθυνου προστασίας προσωπικών δεδομένων.

Στην ερώτηση για το πόσο σημαντική θεωρείται η ύπαρξη ενός υπεύθυνου προστασίας ηλεκτρονικών δεδομένων, ανεξάρτητα από το αν οι συμμετέχοντες έχουν στο χώρο τους έναν σχετικό υπεύθυνο, περίπου τα 2/3 των συμμετεχόντων κατέδειξαν ότι είναι πολύ σημαντική η παρουσία τους, γεγονός που υποδεικνύει τη σημασία της προστασίας των ηλεκτρονικών δεδομένων, που αφορούν το χώρο της υγείας, ενώ λιγότερο από 1 στους 10 συμμετέχοντες θεωρεί ότι η ύπαρξη του υπεύθυνου προστασίας προσωπικών δεδομένων είναι ήσσονος σημασίας.

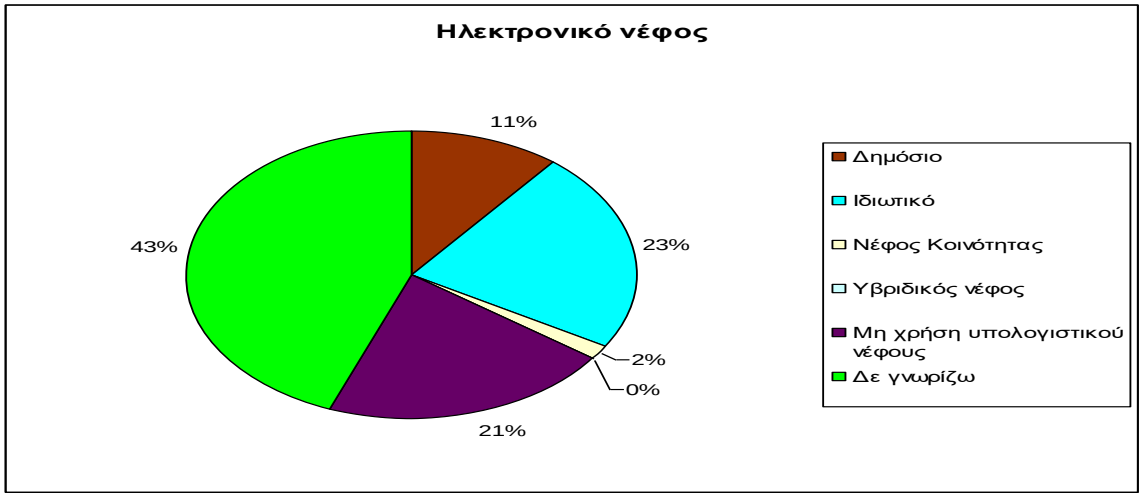


Στην ερώτηση για το ποιος λόγους συλλέγονται ηλεκτρονικά δεδομένα τα 2/3 απάντησαν για τη βελτίωση των παρεχόμενων υπηρεσιών. Φαίνεται ότι οι συμμετέχοντες θεωρούν ότι η συλλογή ηλεκτρονικών δεδομένων τους βοηθάει να καταλάβουν πώς μπορούν να παρέχουν καλύτερες υπηρεσίες, ενώ ένας στους 5 δήλωσε ότι θεωρεί ότι κρατούνται ηλεκτρονικά προσωπικά δεδομένα ασθενών για στατιστικούς λόγους.

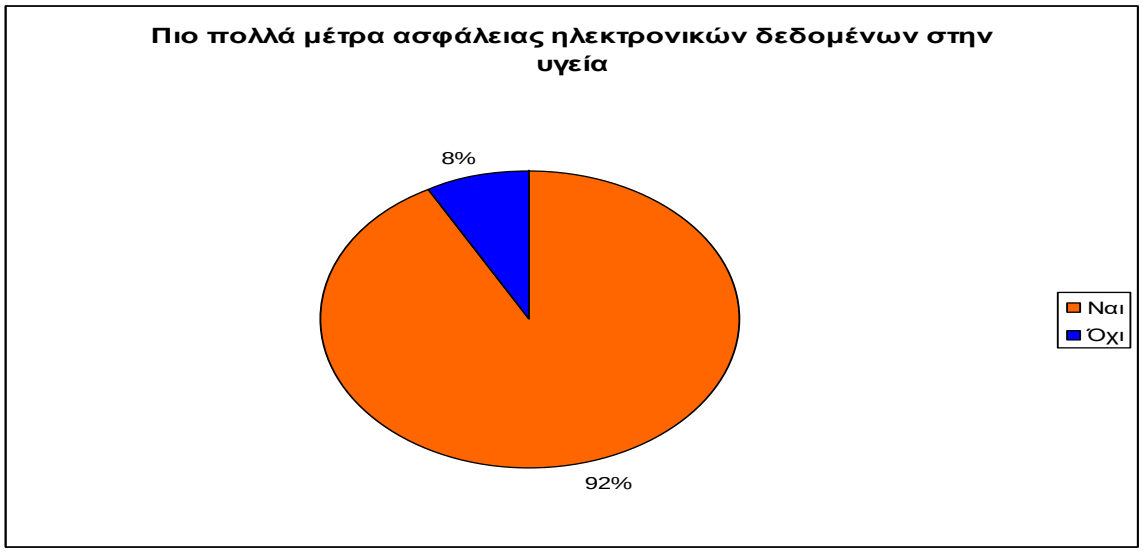


Φαίνεται ότι ανεξάρτητα από το βασικό λόγο για τον οποίο συλλέγονται δεδομένα, οι εργαζόμενοι στο χώρο της υγείας πιστεύουν σε συντριπτικό ποσοστό ότι η συλλογή δεδομένων βοηθάει τη βελτίωση των παρεχόμενων υπηρεσιών στο χώρο της υγείας.

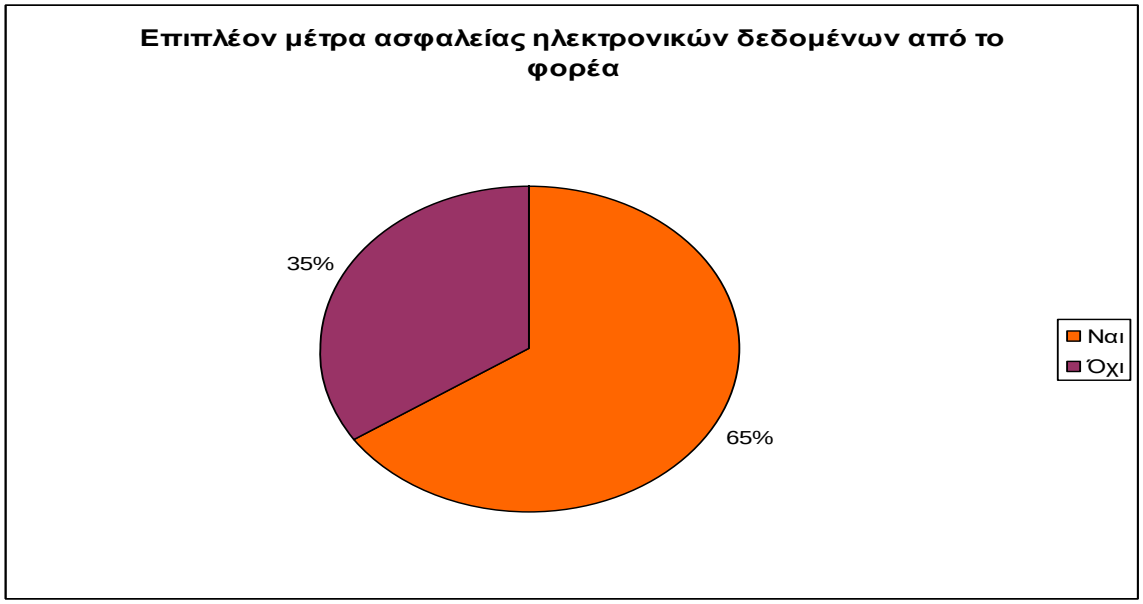
Η επόμενη ερώτηση είχε έναν πιο τεχνικό χαρακτήρα. Πάνω από τα 2/5 των συμμετεχόντων δήλωσαν ότι δε γνωρίζουν τι είδους υπολογιστικό νέφος χρησιμοποιεί το εργασιακό πλαίσιο στο οποίο εργάζονται οι συμμετέχοντες. Μαζί με αυτούς που δήλωσαν ότι δε χρησιμοποιείται κάποιου είδους υπολογιστικό νέφος το ποσοστό των συμμετεχόντων φτάνει σχεδόν τα 2/3 των συμμετεχόντων. Κανένας από τους συμμετέχοντες δε δήλωσε ότι χρησιμοποιείται υβριδικό νέφος.



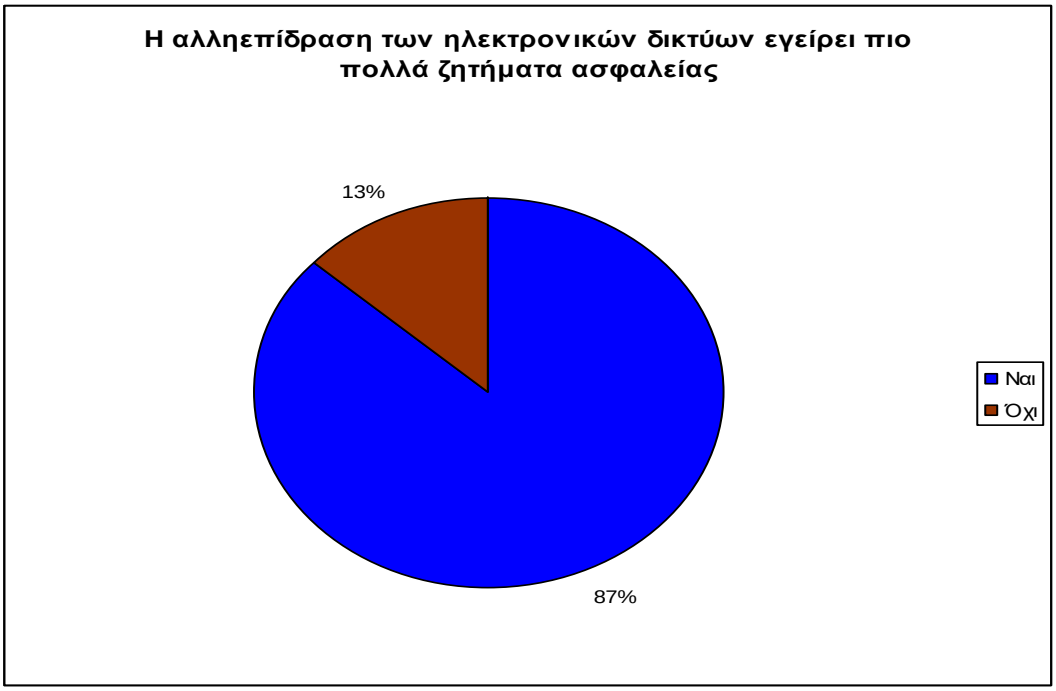
Η συντριπτική πλειοψηφία των συμμετεχόντων, πάνω από 9 στους 10, θεωρεί ότι ο χώρος της υγείας έχει ιδιαιτερότητες και ως εκ τούτου θα πρέπει να λαμβάνονται ισχυρότερα μέτρα σε σχέση με την προστασία των ηλεκτρονικών δεδομένων που χρησιμοποιούνται στο πλαίσιο αυτό.



Εκτός από τη θεωρητική θέση των εργαζόμενων στο χώρο της υγείας τα 2/3 των συμμετεχόντων θεωρούν ότι στην πράξη ότι ο υγειονομικός φορέας στον οποίο εργάζονται θα πρέπει να πάρει περισσότερα μέτρα για την ασφάλεια των ηλεκτρονικών δεδομένων που συλλέγονται, προκειμένου να αποτραπούν δυσάρεστα επακόλουθα.



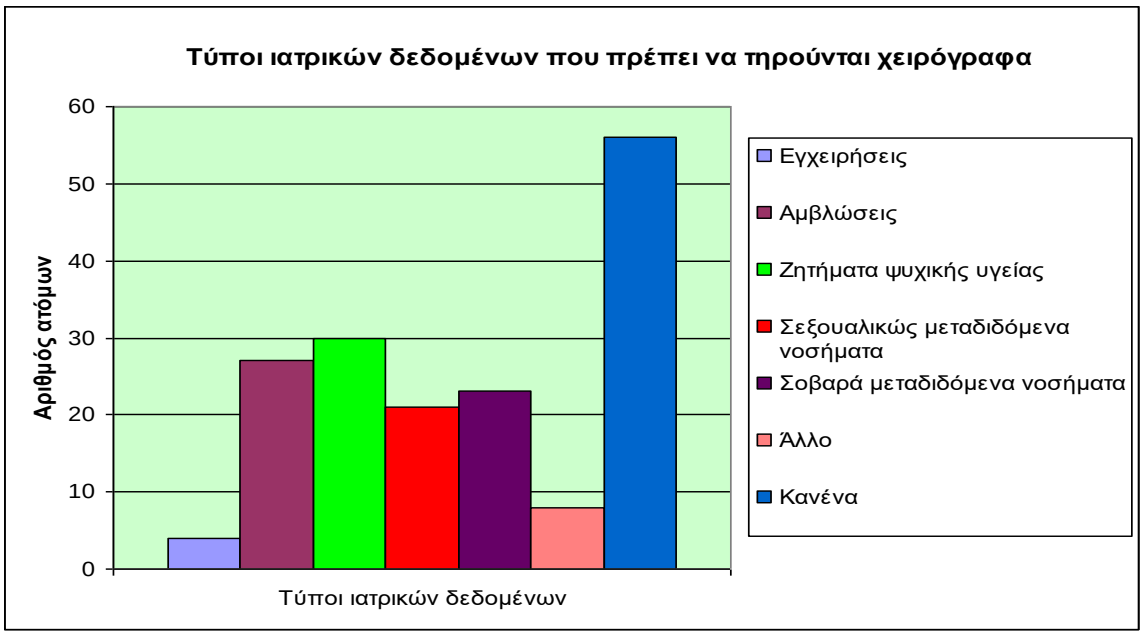
Το γεγονός ότι τα δίκτυα που αφορούν τα μεγάλα ηλεκτρονικά δεδομένα δεν είναι απομονωμένα μεταξύ τους ανησυχεί αρκετούς συμμετέχοντες. Σχεδόν το 90% των συμμετεχόντων θεωρεί ότι αυτό αυξάνει πιθανή διαρροή ηλεκτρονικών δεδομένων.



Τα 2/3 των συμμετεχόντων θεωρούν ότι δεν υπάρχει κάποιος τύπος πληροφοριών που θα έπρεπε να κρατούνται μόνο χειρόγραφα, παρά την εμπιστευτικότητα και την τήρηση του απορρήτου σε πολλά επαγγέλματα υγείας.

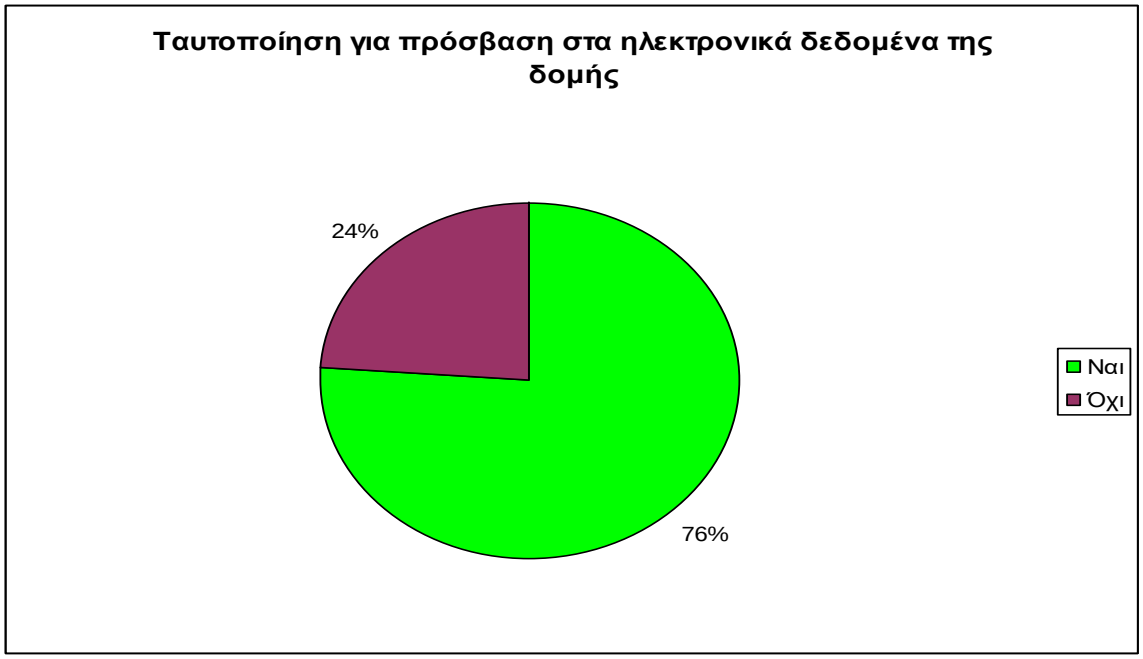
Η τάση να μην τηρούνται κάποιες πληροφορίες χειρόγραφα συνεχίστηκε και στην επόμενη ερώτηση, όπου οι μισοί συμμετέχοντες απάντησαν ότι δε θα πρέπει να τηρείται

χειρόγραφα κανενός είδους πληροφορία. Ένα σημαντικό ποσοστό επικεντρώνεται στα ζητήματα ψυχικής υγείας, μετά στις εκτρώσεις/ αμβλώσεις και μετά στα υπόλοιπα. Η ερώτηση αυτή ήταν η μόνη στην οποία οι συμμετέχοντες μπορούσαν να επιλέξουν ταυτόχρονα περισσότερες από μια επιλογές.

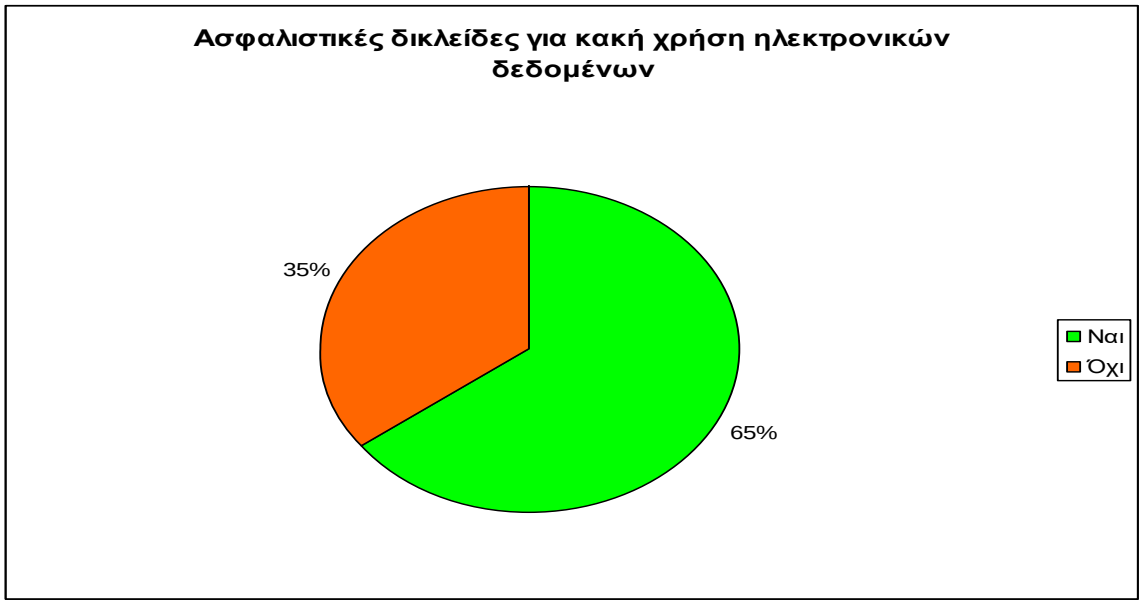


Σε σχέση με το είδος των δεδομένων που ανακτώνται από τις ηλεκτρονικές βάσεις οι απαντήσεις δεν έδειξαν μια συγκεκριμένη ισχυρή τάση. Τα αποτελέσματα διαγνωστικών εξετάσεων είναι τα πιο συχνά δεδομένα που θέλουν να αντλήσουν από τις ηλεκτρονικές βάσεις δεδομένων οι εργαζόμενοι στους χώρους υγείας, καθώς και αν το άτομο υπήρξε σε καραντίνα, αν υπήρξαν/ υπάρχουν ζητήματα ψυχικής υγείας. τα δημογραφικά και το ιστορικό του ασθενούς, η τρέχουσα φαρμακευτική αγωγή και η ύπαρξη ακτινογραφίας.

Περισσότερο από τα 3/4 των ερωτηθέντων δήλωσαν ότι υπάρχει κάποιου είδος ταυτοποίηση για την πρόσβαση στα ηλεκτρονικά δεδομένα του φορέα στον οποίο εργάζονται. Αυτό σημαίνει ότι λόγω της σημασίας της προστασίας των ηλεκτρονικών δεδομένων στους χώρους υγείας υπάρχει ταυτοποίηση προκειμένου να υπάρχει πρόσβαση κάποιου εργαζόμενου στο ηλεκτρονικό σύστημα καταγραφής δεδομένων.



Περίπου τα 2/3 των ερωτηθέντων δήλωσαν ότι υπάρχουν κάποιες επιπλέον ασφαλιστικές δικλείδες στο εργασιακό τους πλαίσιο, ώστε να μην υπάρξει κακή χρήση των ηλεκτρονικών δεδομένων που συγκεντρώνει η δομή υγείας από κάποιο εξουσιοδοτημένο άτομο. Αυτό υποδεικνύει, συνδυαστικά με την προηγούμενη ερώτηση, ότι κάποιες δομές υγείας λαμβάνουν μέτρα προστασίας και από εσωτερικές και από εξωτερικές κακόβουλες προθέσεις.



3.3.2. Επαγωγική στατιστική

3.3.2.α Υποθέσεις

1) α. Ο τύπος του επαγγελματικού πλαισίου θα επηρεάζει την ύπαρξη DPO.

β. Η χώρα κατοικίας θα επηρεάζει την ύπαρξη DPO.

γ. Το ακαδημαϊκό επίπεδο θα επηρεάζει την ύπαρξη DPO.

δ. Η επαγγελματική κατηγορία θα επηρεάζει την ύπαρξη DPO

Φαίνεται ότι ο τύπος πλαισίου επηρεάζει την ύπαρξη υπεύθυνου προστασίας ηλεκτρονικών δεδομένων σύμφωνα με τον έλεγχο χ^2 (4)=11.62, p=.02. Με τη χρήση εκ των υστέρων ελέγχων βρέθηκε ό,τι στατιστικά υπάρχει διαφορά στην ύπαρξη DPO στους εργαζόμενους στις ατομικές επιχειρήσεις (σαφώς περισσότεροι εργαζόμενοι δεν έχουν DPO) και στους εργαζόμενους στο νοσοκομείο (σαφώς περισσότεροι εργαζόμενοι έχουν DPO). Επιβεβαιώθηκε η υπόθεση 1α ότι ο τύπος του επαγγελματικού πλαισίου σχετίζεται με την ύπαρξη DPO.

Σύμφωνα με τον έλεγχο χ^2 η χώρα κατοικίας δεν συσχετίζεται στατιστικά σημαντικά με την ύπαρξη DPO χ^2 (2)=5.52, p=.06.

Το ακαδημαϊκό επίπεδο σχετίζεται στατιστικά σημαντικά με την ύπαρξη DPO σύμφωνα με τον έλεγχο χ^2 (3)=13.79, p=.00. Με βάση των εκ των υστέρων έλεγχο φάνηκε ότι οι κάτοχοι μεταπτυχιακού δουλεύουν πιο συχνά σε δομές χωρίς υπεύθυνο προστασίας προσωπικών δεδομένων ενώ οι απόφοιτοι των ΙΕΚ δουλεύουν με υπεύθυνο προστασίας προσωπικών δεδομένων. Αυτό ίσως εξηγείται με βάση την κείμενη νομοθεσία. Σύμφωνα με αυτήν σε πολλές υγειονομικές ειδικότητες των ΙΕΚ (για παράδειγμα βοηθοί φυσικοθεραπείας, εργοθεραπείας,) δεν επιτρέπεται στους αποφοίτους τους να ανοίξουν δικιά τους επιχείρηση, οπότε οι απόφοιτοι των ΙΕΚ βρίσκουν εργασία σε μεγαλύτερους εργασιακούς χώρους που είναι πιθανότερο να έχουν υπεύθυνο προστασίας δεδομένων.

Σύμφωνα με τον έλεγχο χ^2 η την ύπαρξη DPO η επαγγελματική κατηγορία δεν συσχετίζεται στατιστικά σημαντικά με την ύπαρξη DPO χ^2 (3)=2.22, p=.33.

Οι υποθέσεις 1α και 1γ επιβεβαιωθήκαν. Οι υποθέσεις 1β και 1δ δεν επιβεβαιώθηκαν.

2) α. Ο τύπος του πλαισίου θα επηρεάζει την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα.
β. Η χώρα κατοικίας θα επηρεάζει την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα.
γ. Η ύπαρξη παιδιών θα επηρεάζει την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα.
δ. Η επαγγελματική κατηγορία θα επηρεάζει την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα.
ε. Το ακαδημαϊκό επίπεδο θα επηρεάζει την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα.
στ. Το φύλο θα επηρεάζει την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα.

Ο τύπος πλαισίου σύμφωνα με τον έλεγχο χ^2 (4)=6.25, p=.18. δε σχετίζεται στατιστικά σημαντικά με την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα.

Η χώρα κατοικίας σύμφωνα με τον έλεγχο χ^2 (2)=6.22, p=.045 σχετίζεται στατιστικά σημαντικά με την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα. Με τη χρήση εκ των υστέρων ελέγχων βρέθηκε ό,τι στατιστικά υπάρχει διαφορά αναφορικά με τους διαμένοντες στον Καναδά. Όλοι συμμετέχοντες που διαμένουν στον Καναδά πιστεύουν ότι κάποια είδη πληροφοριών θα πρέπει να κρατούνται χειρόγραφα.

Η ύπαρξη παιδιών σύμφωνα με τον έλεγχο χ^2 (1)=.00, p=.96. δε σχετίζεται στατιστικά σημαντικά με την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα. Η επαγγελματική κατηγορία δε σχετίζεται στατιστικά σημαντικά με την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα σύμφωνα με τον έλεγχο χ^2 (3)=2.4, p=.49.Το ακαδημαϊκό επίπεδο σύμφωνα με τον έλεγχο χ^2 (3)=3.56, p=.31 δεν σχετίζεται στατιστικά σημαντικά με την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα. Το φύλο σύμφωνα με τον έλεγχο χ^2 (1)=.09, p=.77 δε σχετίζεται στατιστικά σημαντικά με την άποψη ότι καμία πληροφορία δε θα έπρεπε να κρατείται χειρόγραφα.

Δεν επιβεβαιώθηκαν οι υποθέσεις 2α,2γ,2δ,2ε και 2στ σε αντίθεση με τη 2β.

3) α. Η χώρα κατοικίας θα επηρεάσει την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου.
β. Το φύλο θα επηρεάσει την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου.
γ. Η επαγγελματική κατηγορία θα επηρεάσει την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου
δ. Το ακαδημαϊκό επίπεδο θα επηρεάσει την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου
ε. Το επαγγελματικό πλαίσιο θα επηρεάσει την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου

Η χώρα κατοικίας σύμφωνα με τον έλεγχο χ^2 (4)=1.38, p=.85 δε σχετίζεται στατιστικά σημαντικά με την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου.

Το φύλο σύμφωνα με τον έλεγχο χ^2 (2)=2.96, p=.23 δε σχετίζεται στατιστικά σημαντικά με την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου.

Η επαγγελματική κατηγορία σύμφωνα με τον έλεγχο χ^2 (6)=6.48, p=.37 δε σχετίζεται στατιστικά σημαντικά με την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου.

Το ακαδημαϊκό επίπεδο σύμφωνα με τον έλεγχο χ^2 (6)=1.66, p=.95 δε σχετίζεται στατιστικά σημαντικά με την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου.

Το επαγγελματικό πλαίσιο σύμφωνα με τον έλεγχο χ^2 (8)=4.87, p=.77 δε σχετίζεται σημαντικά με την αντιλαμβανόμενη συμβολή του DPO στην ασφάλεια των ηλεκτρονικών δεδομένων του ηλεκτρονικού πλαισίου.

Όπως φαίνεται καμία από τις υποθέσεις 3α, 3β, 3γ, 3δ και 3ε δεν επιβεβαιώθηκε.

4) α. Η χώρα κατοικίας θα επηρεάσει το λόγο συλλογής ηλεκτρονικών δεδομένων.
β. Το επαγγελματικό πλαίσιο θα επηρεάσει το λόγο συλλογής ηλεκτρονικών δεδομένων.
γ. Η επαγγελματική κατηγορία θα επηρεάσει το λόγο συλλογής ηλεκτρονικών δεδομένων.
δ. Το ακαδημαϊκό επίπεδο θα επηρεάσει το λόγο συλλογής ηλεκτρονικών δεδομένων.

Η χώρα κατοικίας σύμφωνα με τον έλεγχο χ^2 (6)=3.43, p=.75 δεν σχετίζεται στατιστικά σημαντικά με το λόγο συλλογής ηλεκτρονικών δεδομένων. Το επαγγελματικό πλαίσιο σύμφωνα με τον έλεγχο χ^2 (12)=11.22, p=.51 δεν σχετίζεται στατιστικά σημαντικά με το λόγο συλλογής ηλεκτρονικών δεδομένων. Η επαγγελματική κατηγορία σύμφωνα με τον έλεγχο χ^2 (9)=7.77, p=.56 δεν σχετίζεται στατιστικά σημαντικά με το λόγο συλλογής ηλεκτρονικών δεδομένων. Το ακαδημαϊκό επίπεδο σύμφωνα με τον έλεγχο χ^2 (9)=10.86, p=.29 δεν σχετίζεται στατιστικά σημαντικά με το λόγο συλλογής ηλεκτρονικών δεδομένων.

Οι υποθέσεις 4α, 4β, 4γ και 4δ δεν επιβεβαιωθήκαν.

5) α. Η χώρα κατοικίας επηρεάζει την αντιλαμβανόμενη βελτίωση υπηρεσιών από τη συλλογή ηλεκτρονικών δεδομένων.

β. Ο τύπος πλαισίου επηρεάζει την αντιλαμβανόμενη βελτίωση υπηρεσιών από τη συλλογή ηλεκτρονικών δεδομένων.

γ. Η επαγγελματική κατηγορία επηρεάζει την αντιλαμβανόμενη βελτίωση υπηρεσιών από τη συλλογή ηλεκτρονικών δεδομένων.

δ. Το ακαδημαϊκό επίπεδο επηρεάζει την αντιλαμβανόμενη βελτίωση υπηρεσιών από τη συλλογή ηλεκτρονικών δεδομένων.

Η χώρα σύμφωνα με τον έλεγχο χ^2 (2)=3.61, p=.16 δε σχετίζεται στατιστικά σημαντικά με την αντιλαμβανόμενη βελτίωση υπηρεσιών από τη συλλογή ηλεκτρονικών δεδομένων. Το επαγγελματικό πλαίσιο σύμφωνα με τον έλεγχο χ^2 (4)=4.83, p=.31 δε σχετίζεται στατιστικά σημαντικά με την αντιλαμβανόμενη βελτίωση υπηρεσιών από τη συλλογή ηλεκτρονικών δεδομένων. Η επαγγελματική κατηγορία σύμφωνα με τον έλεγχο χ^2 (3)=3.09, p=.38. δε σχετίζεται στατιστικά σημαντικά με την αντιλαμβανόμενη βελτίωση υπηρεσιών από τη συλλογή ηλεκτρονικών δεδομένων Το ακαδημαϊκό επίπεδο σύμφωνα με τον έλεγχο χ^2 (3)=2.8, p=.42 δε σχετίζεται στατιστικά σημαντικά με την αντιλαμβανόμενη βελτίωση υπηρεσιών από τη συλλογή ηλεκτρονικών δεδομένων

Οι υποθέσεις 5α, 5β, 5γ, και 5δ δεν επιβεβαιώθηκαν.

6) α. Η χώρα κατοικίας επηρεάζει την ύπαρξη και τον τύπο του ηλεκτρονικού νέφους που έχει ο εργαζόμενος στο χώρο εργασίας του.

β. Ο τύπος πλαισίου επηρεάζει την ύπαρξη και τον τύπο του ηλεκτρονικού νέφους που έχει ο εργαζόμενος στο χώρο εργασίας του.

γ. Η επαγγελματική κατηγορία επηρεάζει την ύπαρξη και τον τύπο του ηλεκτρονικού νέφους που έχει ο εργαζόμενος στο χώρο εργασίας του.

δ. Το ακαδημαϊκό επίπεδο επηρεάζει την ύπαρξη και τον τύπο του ηλεκτρονικού νέφους που έχει ο εργαζόμενος στο χώρο εργασίας του.

Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ χώρας κατοικίας και της ύπαρξης και του τύπου του ηλεκτρονικού νέφους που έχει ο εργαζόμενος στο χώρο εργασίας του σύμφωνα με τον έλεγχο χ^2 (8)=6.44, p=.6.

Υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ επαγγελματικού πλαισίου και του τύπου του ηλεκτρονικού νέφους που έχει ο εργαζόμενος στο χώρο εργασίας του χ^2 (16)=28.13, p=.03. Από τον εκ των υστερών έλεγχο φαίνεται ότι η έλλειψη ύπαρξης νέφους αλλάζει στατιστικά σημαντικά σε σχέση με τις κατηγορίες του εργασιακού πλαισίου.

Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ επαγγελματικής κατηγορίας και του τύπου του ηλεκτρονικού νέφους που έχει ο εργαζόμενος στο χώρο εργασίας του χ^2 (12)=12.6, p=.4.

Υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ ακαδημαϊκού επιπέδου και του τύπου του ηλεκτρονικού νέφους που έχει ο εργαζόμενος στο χώρο εργασίας του χ^2 (12)=32.28, p=.00. Μετά των εκ των υστέρων έλεγχο φάνηκε ότι στατιστικά στα περισσότερα εργασιακά πλαίσια που εργάζονται απόφοιτοι των ΙΕΚ χρησιμοποιούν ιδιωτικό νέφος.

Οι υποθέσεις 6α και 6γ δεν επιβεβαιώθηκαν. Οι υποθέσεις 6β και 6δ επιβεβαιώθηκαν.

7) α. Η χώρα κατοικίας επηρεάζει την ύπαρξη της άποψης ότι οι φορείς υγείας πρέπει να παίρνουν περισσότερα μέτρα.
β. Ο τύπος πλαισίου επηρεάζει την ύπαρξη της άποψης ότι οι φορείς υγείας πρέπει να παίρνουν περισσότερα μέτρα.
γ. Η επαγγελματική κατηγορία επηρεάζει την ύπαρξη της άποψης ότι οι φορείς υγείας πρέπει να παίρνουν περισσότερα μέτρα.
δ. Το ακαδημαϊκό επίπεδο επηρεάζει την ύπαρξη της άποψης ότι οι φορείς υγείας πρέπει να παίρνουν περισσότερα μέτρα.

Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ χώρας κατοικίας και της άποψης ότι οι φορείς υγείας πρέπει να παίρνουν περισσότερα μέτρα σύμφωνα με τον έλεγχο χ^2 (2)=1.85, p=.4. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ τύπου επαγγελματικού πλαισίου και της άποψης ότι οι φορείς υγείας πρέπει να παίρνουν περισσότερα μέτρα σύμφωνα με τον έλεγχο χ^2 (4)=2.46, p=.65. Δεν υπάρχει στατιστικά συσχέτιση μεταξύ επαγγελματικής κατηγορίας και της άποψης ότι οι φορείς υγείας πρέπει να παίρνουν περισσότερα μέτρα σύμφωνα με τον έλεγχο χ^2 (3)=2.88, p=.41.
Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ ακαδημαϊκού επιπέδου και της άποψης ότι οι φορείς υγείας πρέπει να παίρνουν περισσότερα μέτρα σύμφωνα με τον έλεγχο χ^2 (3)=.75, p=.86.

Δεν επιβεβαιώθηκε κάποια από τις υποθέσεις 7α, 7β, 7γ και 7δ.

8) α. Η χώρα κατοικίας επηρεάζει το αν εργάζονται σε φορείς υγείας που έχουν παίρνουν περισσότερα μέτρα για την ασφάλεια των ηλεκτρονικών δεδομένων.
β. Ο τύπος πλαισίου επηρεάζει το αν εργάζονται σε φορείς υγείας που έχουν παίρνουν περισσότερα μέτρα για την ασφάλεια των ηλεκτρονικών δεδομένων.
γ. Η επαγγελματική κατηγορία επηρεάζει το αν εργάζονται σε φορείς υγείας που έχουν παίρνουν περισσότερα μέτρα για την ασφάλεια των ηλεκτρονικών δεδομένων.
δ. Το ακαδημαϊκό επίπεδο επηρεάζει το αν εργάζονται σε φορείς υγείας που έχουν παίρνουν περισσότερα μέτρα για την ασφάλεια των ηλεκτρονικών δεδομένων.

Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ χώρας κατοικίας και το αν εργάζονται σε φορείς υγείας που παίρνουν περισσότερα μέτρα για την ασφάλεια των ηλεκτρονικών δεδομένων σύμφωνα με τον έλεγχο χ^2 (2)=2.2, p=.33. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ επαγγελματικού πλαισίου και το αν εργάζονται σε φορείς υγείας που παίρνουν περισσότερα μέτρα για την ασφάλεια των ηλεκτρονικών δεδομένων σύμφωνα με τον έλεγχο χ^2 (4)=5, p=.29. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ επαγγελματικής κατηγορίας και το αν εργάζονται σε φορείς υγείας που παίρνουν περισσότερα μέτρα για την ασφάλεια των ηλεκτρονικών δεδομένων

σύμφωνα με τον έλεγχο χ^2 (3)=6.32, p=.1. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ ακαδημαϊκού επίπεδου και το αν εργάζονται σε φορείς υγείας που παίρνουν περισσότερα μέτρα για την ασφάλεια των ηλεκτρονικών δεδομένων σύμφωνα με τον έλεγχο χ^2 (3)=.55, p=.91.

Δεν επιβεβαιώθηκε κάποια από τις υποθέσεις 8α, 8β, 8γ και 8δ.

9) α. Η χώρα κατοικίας επηρεάζει το αν θεωρούν ότι η συγχώνευση δικτύων εγείρει περισσότερα συστήματα ασφάλειας.
β. Ο τύπος πλαισίου επηρεάζει το αν θεωρούν ότι η συγχώνευση δικτύων εγείρει περισσότερα συστήματα ασφάλειας.
γ. Η επαγγελματική κατηγορία επηρεάζει το αν θεωρούν ότι η συγχώνευση δικτύων εγείρει περισσότερα συστήματα ασφάλειας.
δ. Το ακαδημαϊκό επίπεδο επηρεάζει το αν θεωρούν ότι η συγχώνευση δικτύων εγείρει περισσότερα συστήματα ασφάλειας.

Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ χώρας κατοικίας και το αν θεωρούν ότι η συγχώνευση δικτύων εγείρει περισσότερα συστήματα ασφάλειας χ^2 (2)=.5, p=.78. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ τύπου επαγγελματικού πλαισίου και το αν θεωρούν ότι η συγχώνευση δικτύων εγείρει περισσότερα συστήματα ασφάλειας χ^2 (4)=1.6, p=.81. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ χώρας επαγγελματικής κατηγορίας και το αν θεωρούν ότι η συγχώνευση δικτύων εγείρει περισσότερα συστήματα ασφάλειας χ^2 (3)=.84, p=.84.Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ ακαδημαϊκού επιπέδου και το αν θεωρούν ότι η συγχώνευση δικτύων εγείρει περισσότερα συστήματα ασφάλειας χ^2 (3)=1.3, p=.73.

Δεν επιβεβαιώθηκε κάποια από τις υποθέσεις 9α, 9β, 9γ και 9δ.

10) α. Η χώρα κατοικίας επηρεάζει το αν εργάζονται σε φορείς υγείας που ζητούν ταυτοποίηση για την είσοδο στο ηλεκτρονικό σύστημα καταγραφής δεδομένων.

β. Ο τύπος πλαισίου επηρεάζει το αν εργάζονται σε φορείς υγείας που ζητούν ταυτοποίηση για την είσοδο στο ηλεκτρονικό σύστημα καταγραφής δεδομένων.
γ. Η επαγγελματική κατηγορία επηρεάζει το αν εργάζονται σε φορείς υγείας που ζητούν ταυτοποίηση για την είσοδο στο ηλεκτρονικό σύστημα καταγραφής δεδομένων.
δ. Το ακαδημαϊκό επίπεδο επηρεάζει το αν εργάζονται σε φορείς υγείας που ζητούν ταυτοποίηση για την είσοδο στο ηλεκτρονικό σύστημα καταγραφής δεδομένων.

Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ χώρας κατοικίας και το αν ο φορέας υγείας ζητάει ταυτοποίηση για την είσοδο στο ηλεκτρονικό σύστημα καταγραφής δεδομένων σύμφωνα με τον έλεγχο χ^2 (2)=3.45, p=.18. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ επαγγελματικού πλαισίου και το αν ο φορέας υγείας ζητάει ταυτοποίηση για την είσοδο στο ηλεκτρονικό σύστημα καταγραφής δεδομένων σύμφωνα με τον έλεγχο χ^2 (4)=5.3, p=.26. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ επαγγελματικής κατηγορίας και το αν ο φορέας υγείας ζητάει ταυτοποίηση για την είσοδο στο ηλεκτρονικό σύστημα καταγραφής δεδομένων σύμφωνα με τον έλεγχο χ^2 (3)=2.26, p=.52. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ ακαδημαϊκού επιπέδου και το αν ο φορέας υγείας ζητάει ταυτοποίηση για την είσοδο στο ηλεκτρονικό σύστημα καταγραφής δεδομένων σύμφωνα με τον έλεγχο χ^2 (3)=.99, p=.8.

Δεν επιβεβαιώθηκε κάποια από τις υποθέσεις 10α, 10β, 10γ και 10δ.

11) α. Η χώρα κατοικίας επηρεάζει το αν εργάζονται σε φορείς υγείας που έχουν επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους
β. Ο τύπος πλαισίου επηρεάζει το αν εργάζονται σε φορείς υγείας που έχουν επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους
γ. Η επαγγελματική κατηγορία επηρεάζει το αν εργάζονται σε φορείς υγείας που έχουν επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους

δ. Το ακαδημαϊκό επίπεδο επηρεάζει το αν εργάζονται σε φορείς υγείας που έχουν επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους.

Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ χώρας κατοικίας και το αν εργάζονται σε φορείς υγείας που έχουν επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους σύμφωνα με τον έλεγχο χ^2 (2)=2.79, p=.25. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ τύπου επαγγελτικού πλαισίου και το αν εργάζονται σε συγκεκριμένους φορείς υγείας που έχουν επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους σύμφωνα με τον έλεγχο χ^2 (4)=6.6, p=.16. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ επαγγελματικής κατηγορίας και το αν εργάζονται σε φορείς υγείας που έχουν επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους σύμφωνα με τον έλεγχο χ^2 (3)=2.13, p=.55. Δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ ακαδημαϊκού επιπέδου και το αν εργάζονται σε φορείς υγείας που έχουν επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους σύμφωνα με τον έλεγχο χ^2 (3)=4.46, p=.22.

Δεν επιβεβαιώθηκε κάποια από τις υποθέσεις 11α, 11β, 11γ και 11δ.

3.3.2.β Υποθέσεις για τις κύριες επιδράσεις ηλικίας και χρόνων προϋπηρεσίας και τη συσχέτιση μεταξύ κατηγορικών μεταβλητών

Για να διαπιστώσουμε τις επιδράσεις της ηλικίας στις ειδικές ερωτήσεις του ερωτηματολογίου διεξαγάγαμε το μη παραμετρικό έλεγχο Kruskal Wallis, λόγω της μη κανονικής κατανομής των μεταβλητών..

Σύμφωνα με τον έλεγχο Kruskal Wallis η ηλικία δεν επηρεάζει την αντιλαμβανόμενη βελτίωση εργασίας από τη συλλογή ηλεκτρονικών δεδομένων χ^2 (4)=2.76, p=.6. Σύμφωνα με τον έλεγχο Kruskal Wallis η ηλικία δεν επηρεάζει την

ύπαρξη νέφους ή το είδος του νέφους που έχει ο συμμετέχων στο χώρο εργασίας του χ^2 (4)=.155, p=.82. Σύμφωνα με τον έλεγχο Kruskal Wallis η ηλικία δεν επηρεάζει τη γνώμη των συμμετεχόντων για τη λήψη πιο πολλών μέτρων ασφαλείας για τα δεδομένα που συλλέγονται ηλεκτρονικά χ^2 (4)=1.34, p=.86. Σύμφωνα με τον έλεγχο Kruskal Wallis η ηλικία δεν επηρεάζει το αν οι συμμετέχοντες εργάζονται σε ένα πλαίσιο που έχει λάβει πιο πολλά μέτρα ασφαλείας για τα δεδομένα που συλλέγονται ηλεκτρονικά χ^2 (4)=7.6, p=.11. Σύμφωνα με τον έλεγχο Kruskal Wallis η ηλικία δεν επηρεάζει το αν οι συμμετέχοντες θεωρούν ότι με τη συγχώνευση των δικτύων που επεξεργάζονται τα ηλεκτρονικά δεδομένα εγείρουν περισσότερα ζητήματα ασφαλείας χ^2 (4)=5.32, p=.26.
Σύμφωνα με τον έλεγχο Kruskal Wallis η ηλικία δεν επηρεάζει το αν οι συμμετέχοντες εργάζονται σε ένα πλαίσιο που έχει μεθόδους ταυτοποίησης προκειμένου οι εργαζόμενοι να έχουν πρόσβαση στα ηλεκτρονικά δεδομένων των ασθενών χ^2 (4)=4.84, p=.3.
Σύμφωνα με τον έλεγχο Kruskal Wallis η ηλικία δεν επηρεάζει το αν οι συμμετέχοντες εργάζονται σε ένα πλαίσιο που έχει επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους χ^2 (4)=4.73, p=.32.

Η ηλικία φάνηκε να μην έχει στατιστικά σημαντική επίδραση σε κάποια από τις ειδικές ερωτήσεις του ερωτηματολογίου.

Για να διαπιστώσουμε τις επιδράσεις των χρόνων προϋπηρεσίας στις ειδικές ερωτήσεις του ερωτηματολογίου διεξαγάγαμε το μη παραμετρικό έλεγχο Kruskal Wallis, λόγω της μη κανονικής κατανομής των μεταβλητών.

Σύμφωνα με τον έλεγχο Kruskal Wallis τα χρόνια προϋπηρεσίας δεν επηρεάζουν την αντιλαμβανόμενη βελτίωση εργασίας από τη συλλογή ηλεκτρονικών δεδομένων χ^2 (4)=2.34, p=.67. Σύμφωνα με τον έλεγχο Kruskal Wallis τα χρόνια προϋπηρεσίας δεν επηρεάζουν την ύπαρξη νέφους ή το είδος του νέφους που έχει ο συμμετέχων στο χώρο εργασίας του χ^2 (4)=1.03, p=.91. Σύμφωνα με τον έλεγχο Kruskal Wallis τα χρόνια προϋπηρεσίας δεν επηρεάζουν τη γνώμη των συμμετεχόντων για τη λήψη πιο πολλών μέτρων ασφαλείας για τα δεδομένα που συλλέγονται ηλεκτρονικά χ^2 (4)=4.21, p=.38.

Σύμφωνα με τον έλεγχο Kruskal Wallis τα χρόνια προϋπηρεσίας δεν επηρεάζουν το αν οι συμμετέχοντες εργάζονται σε ένα πλαίσιο που έχει λάβει πιο πολλά μέτρα ασφαλείας για τα δεδομένα που συλλέγονται ηλεκτρονικά χ^2 (4)=2.9, p=.57. Σύμφωνα με τον έλεγχο Kruskal Wallis τα χρόνια προϋπηρεσίας δεν επηρεάζουν το αν οι συμμετέχοντες θεωρούν ότι με τη συγχώνευση των δικτύων που επεξεργάζονται τα ηλεκτρονικά δεδομένα εγείρουν περισσότερα ζητήματα ασφαλείας χ^2 (4)=6.13, p=.19.

Σύμφωνα με τον έλεγχο Kruskal Wallis τα χρόνια προϋπηρεσίας επηρεάζουν το αν οι συμμετέχοντες εργάζονται σε ένα πλαίσιο που έχει μεθόδους ταυτοποίησης προκειμένου οι εργαζόμενοι να έχουν πρόσβαση στα ηλεκτρονικά δεδομένων των ασθενών χ^2 (8)=11.1, p=.03.

Σύμφωνα με των εκ των υστέρων έλεγχο φάνηκε ότι υπάρχει στατιστικά σημαντική διαφοροποίηση μεταξύ των ομάδων 5-9 έτη προϋπηρεσίας και πάνω από 20 έτη προϋπηρεσίας. Οι εργαζόμενοι με πάνω από 20 έτη προϋπηρεσίας εργάζονται πιο συχνά σε δομές που ζητούν ταυτοποίηση για την πρόσβαση στο ηλεκτρονικό σύστημα σε σχέση με εργαζόμενους που έχουν 5-9 έτη προϋπηρεσίας.

Σύμφωνα με τον έλεγχο Kruskal Wallis τα χρόνια προϋπηρεσίας δεν επηρεάζουν το αν οι συμμετέχοντες εργάζονται σε ένα πλαίσιο που έχει επιπλέον ασφαλιστικές δικλείδες για την κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους του εργασιακού πλαισίου χ^2 (4) 6.11, p=.19.

Φάνηκε ότι τα έτη προϋπηρεσίας των συμμετεχόντων επηρεάζουν μόνο σε σχέση με την ύπαρξη ταυτοποίησης για την πρόσβαση στο ηλεκτρονικό σύστημα καταγραφής των δεδομένων.

Χρησιμοποιήθηκε ο συντελεστής συσχέτισης του Pearson (r) προκειμένου να φανεί ο βαθμός συμμεταβολής μεταξύ των διάφορων τύπων πληροφοριών που θα μπορούσαν να κρατηθούν χειρόγραφα. Από ότι φαίνεται υπάρχει δυο σημαντικές αρνητικές συσχετίσεις μεταξύ των σεξουαλικώς μεταδιδόμενων νοσημάτων και των

ζητημάτων ψυχικής υγείας(r=-.69) και μεταξύ ζητημάτων ψυχικής υγείας και της επιλογής κανένα (r=-.69) . Γενικώς η επιλογή κανένα συσχετίζεται σημαντικά, με αρνητικό τρόπο, με όλες τις προηγούμενες επιλογές εκτός από την επιλογή σοβαρά μεταδιδόμενα νοσήματα. Η συσχέτιση μεταξύ της επιλογής "κανένα" για τους τύπους των χειρόγραφων δεδομένων και της προηγούμενης ερώτησης για το αν θα έπρεπε γενικά να τηρούνται δεδομένα χειρόγραφα είναι μέτρια (r=-.56). Το αρνητικό πρόσημο της συσχέτισης εξηγείται από τη διαφορετική κωδικοποίηση που έγινε στις 2 μεταβλητές.

3.4 Συμπεράσματα

3.4.1. Περιγραφική στατιστική

Σε επίπεδο περιγραφικής στατιστικής οι γυναίκες ήταν σαφώς περισσότερες από τους άντρες, η μεγάλη πλειοψηφία ήταν από την Ελλάδα, κάτι που αναμενόταν εφόσον η βάση της έρευνας ήταν στην Ελλάδα. Σε σχέση με την ηλικία πάνω από τα 2/3 ήταν μεταξύ 30 και 49 ετών (ηλικιακές κατηγορίες 30-39, 40-49). Το παραϊατρικό προσωπικό ήταν η μεγαλύτερη πληθυσμιακά ομάδα, ενώ και υπόλοιπες ομάδες είχαν σημαντική εκπροσώπηση Η πλειοψηφία των συμμετεχόντων, τα 2/3 περίπου, δουλεύει είτε σε άλλο πλαίσιο είτε σε νοσοκομείο.

Σχεδόν οι μισοί συμμετέχοντες είναι απόφοιτοι τριτοβάθμιας εκπαίδευσης, ενώ το 1/3 είναι κάτοχοι μεταπτυχιακού. Εδώ φαίνεται ότι η πρώτη και η τελευταία ακαδημαϊκή κατηγορία (ΙΕΚ και διδακτορικό) έχουν μικρή εκπροσώπηση στο δείγμα μας.

Η μεγάλη πλειοψηφία του δείγματος είτε δεν έχει παιδιά (περίπου 40%), είτε έχει μέχρι 2 παιδιά. Οι μισοί είναι παντρεμένοι, ενώ το 1/3 των συμμετεχόντων είναι ελεύθεροι. Πάνω από τους μισούς συμμετέχοντες ήταν από τη Θεσσαλονίκη, γεγονός αναμενόμενο εφόσον το προσωπικό που διεξήγαγε την έρευνα καθώς και το εκπαιδευτικό ίδρυμα για την οποία διεξήχθη αυτή, έχουν ως βάση τους τη Θεσσαλονίκη. Σε σχέση με τα έτη επαγγελματικής εμπειρίας οι συμμετέχοντες είναι μοιρασμένοι. Ελαφρώς υψηλότερη εκπροσώπηση έχουν οι εργαζόμενοι με προϋπηρεσία 10-14 έτη.

Ένα σημαντικό ποσοστό των συμμετεχόντων δε γνωρίζει αν στο χώρο εργασίας του χρησιμοποιείται κάποιου είδος υπολογιστικού νέφος και ποιο είναι αυτό, ενώ περίπου 1/5 δήλωσε ότι δε χρησιμοποιείται κάποιου είδους υπολογιστικού νέφους. Σε

σχέση με το είδος των δεδομένων, που συλλέγονται ηλεκτρονικά τα 3/5 λένε ότι χρησιμοποιούν δομημένα ηλεκτρονικά δεδομένα και κυρίως ηλεκτρονικούς φακέλων ασθενών.

Σε γενικές γραμμές περίπου τα 2/3 των συμμετεχόντων θεωρούν πολύ σημαντική την ύπαρξη ενός υπεύθυνου προστασίας προσωπικών δεδομένων στο χώρο της υγείας ,ενώ περίπου οι μισοί έχουν στο εργασιακό τους χώρο υπεύθυνο προστασίας προσωπικών δεδομένων. Λίγοι, ούτε 1 στους 10 συμμετέχοντες, στο χώρο της υγείας θεωρούν ότι είναι μικρή η σημασία της ύπαρξης ενός υπεύθυνου προστασίας προσωπικών δεδομένων γεγονός που καταδεικνύει τη σημασία που αποδίδουν οι εργαζόμενοι στο χώρο της υγείας στην προστασία των ηλεκτρονικών προσωπικών δεδομένων.

Περισσότερο από ένας στους 10 δίνει έμφαση στο γεγονός ότι η συλλογή ηλεκτρονικών δεδομένων θα μπορούσε να αποτρέψει κάποια απάτη, ενώ τα 2/3 των συμμετεχόντων λένε ότι τα ηλεκτρονικά δεδομένα συλλέγονται για τη βελτίωση των υπαρχόντων υπηρεσιών του πλαισίου· η μεγάλη πλειοψηφία των συμμετεχόντων, πάνω από 9/10, θεωρεί ότι όντως η συλλογή ηλεκτρονικών δεδομένων τους βοηθάει να βελτιώσουν τις υπηρεσίες που παρέχουν.

Περίπου 2 στους 3 συμμετέχοντες θεωρούν ότι όλα τα στοιχεία που σχετίζονται με το ιστορικό των ασθενών πρέπει να καταχωρίζονται ηλεκτρονικά. Αυτό υποδηλώνει την πίστη των συμμετεχόντων ότι τα δεδομένα, ανεξαρτήτως της φύσεώς τους, διατηρούνται καλύτερα με την ηλεκτρονική καταχώρισή τους και όχι με τη χειρόγραφη καταγραφή σε καρτέλες. Αυτό συμβαίνει πιθανόν γιατί οι πάροχοι υπηρεσιών υγείας κρίνουν ότι χρειάζονται συνολική γνώση του ιστορικού του θεραπευμένου προκειμένου να προσφέρουν καλύτερες υπηρεσίες υγείας.

Στην επόμενη ερώτηση που ήθελε συγκεκριμενοποίηση του είδους πληροφοριών που θα έπρεπε να τηρούνται χειρόγραφα κάποιοι από τους συμμετέχοντες που είπαν ότι δεν πρέπει να τηρούνται χειρόγραφα πληροφορίες δεν επέλεξαν την επιλογή "κανένα" που προσφερόταν. Σε γενικές γραμμές ζητήματα εκτρώσεων, ψυχικής και σεξουαλικής υγείας και σοβαρών μεταδοτικών νοσημάτων, ανησυχούν μέρος των συμμετεχόντων.

Οι συμμετέχοντες που εργάζονται σε δομές υγείας στην πλειοψηφία τους είτε πιστεύουν ότι θα έπρεπε γενικώς οι δομές υγείας να παίρνουν περισσότερα μέτρα ασφαλείας σε σχέση με τις λοιπές επιχειρήσεις (9 στους 10,) είτε ότι ο συγκεκριμένος φορέας στον οποίο εργάζονται να λάβει κάποια επιπλέον μέτρα (2 στους 3).

Το γεγονός ότι στη σύγχρονη εποχή είναι συγχωνευμένα μεταξύ τους τα δίκτυα που επεξεργάζονται πληροφορίες ανησυχεί πολλούς συμμετέχοντες, πάνω από 9 στους 10 θεωρούν ότι αυτό εγείρει επιπλέον ζητήματα ασφαλείας των ηλεκτρονικών δεδομένων.

Φαίνεται ότι οι δομές υγείας παίρνουν κάποια επιπλέον μέτρα για τη διαρροή των ηλεκτρονικών δεδομένων , δεδομένου ότι πάνω από τα 3/4 των συμμετεχόντων δήλωσαν ότι απαιτείται κάποιου είδους ταυτοποίηση προκειμένου να εισέλθουν στο ηλεκτρονικό σύστημα καταγραφής δεδομένων, ενώ πάνω από τα 2/3 δήλωσαν ότι υπάρχουν και κάποιες περαιτέρω ασφαλιστικές δικλείδες προκειμένου να μη γίνει κακή χρήση των ηλεκτρονικών δεδομένων από τους εργαζόμενους του πλαισίου που εργάζονται.

3.4.2. Επαγωγική στατιστική

Είναι λογικό ο τύπος του εργασιακού πλαισίου να επηρεάζει την ύπαρξη υπεύθυνου προστασίας προσωπικών δεδομένων. Επίσης είναι αναμενόμενο σε μεγάλες δομές όπως είναι τα νοσοκομεία να είναι πιο συχνή η ύπαρξη υπεύθυνου προστασίας προσωπικών δεδομένων σε σχέση με τις ατομικές επιχειρήσεις (όπως τα διάφορα ιδιωτικά γραφεία παραϊατρικών επαγγελμάτων). Είναι δύσκολο για μια ατομική επιχείρηση να επωμιστεί το κόστος ενός επιπλέον υπαλλήλου έστω και μερικής απασχόλησης· επίσης είναι πολύ πιθανόν ο ιδιοκτήτης της ατομικής επιχείρησης να είναι το μόνο άτομο που έχει πρόσβαση στο ηλεκτρονικό σύστημα που τηρεί ηλεκτρονικά αρχεία ωφελούμενων.

Αναφορικά με το αν θα έπρεπε να τηρούνται κάποια είδη πληροφοριών χειρόγραφα, διαφοροποιούνται στατιστικά όλοι οι συμμετέχοντες από τον Καναδά· όλοι τους επεσήμαναν ότι θα έπρεπε κάποιες πληροφορίες να τηρούνται χειρόγραφα, με μια έμφαση στα ζητήματα ψυχικής υγείας.

Οι αναλύσεις για τη σπουδαιότητα του υπεύθυνου προστασίας προσωπικών δεδομένων έδειξαν ότι το μεγάλο ποσοστό των συμμετεχόντων πιστεύει ότι είναι σημαντική η συμβολή και αυτό συμβαίνει ανεξαρτήτως δημογραφικών παραγόντων. Ακόμα η αντιλαμβανόμενη βελτίωση υπηρεσιών από τη συλλογή ηλεκτρονικών δεδομένων ήταν ισχυρή τάση στα δεδομένα μας και δε φάνηκε να επηρεάζεται από συγκεκριμένους δημογραφικούς παράγοντες όπως και ο βασικός λόγος συλλογής ηλεκτρονικών δεδομένων.

Φάνηκε ότι υπάρχει κάποια στατιστικά σημαντική αλληλεπίδραση μεταξύ του τύπου ηλεκτρονικού νέφους και του ακαδημαϊκού επιπέδου των συμμετεχόντων. Οι απόφοιτοι των ΙΕΚ τείνουν να δουλεύουν συχνότερα σε δομές που έχουν ιδιωτικό ηλεκτρονικό νέφος.

Η θεωρητική γνώμη των συμμετεχόντων ότι οι δομές υγείας θα έπρεπε να λαμβάνουν περισσότερα μέτρα ασφαλείας καθώς και η επί του πρακτέου άποψη ότι ο χώρος εργασίας στον οποίο εργάζονται θα πρέπει να λάβει περισσότερα μέτρα ασφαλείας δεν επηρεάζονται από συγκεκριμένους δημογραφικούς παράγοντες. Ακόμα το γεγονός της συγχώνευσης δικτύων και των συνακόλουθων ζητημάτων ασφαλείας, το αν ο χώρος εργασίας έχει μεθόδους ταυτοποίησης για την είσοδο στο ηλεκτρονικό σύστημα δεδομένων και η ύπαρξη επιπλέον ασφαλιστικών δικλείδων για την αποτροπή κακής χρήσης των ηλεκτρονικών δεδομένων από εργαζόμενους του πλαισίου δεν επηρεάζονται από συγκεκριμένους δημογραφικούς παράγοντες.

Αναφορικά με τις κύριες επιδράσεις μεταβλητών η ηλικία φάνηκε να μην έχει επίδραση σε κάποια από τις ειδικές ερωτήσεις του ερωτηματολογίου μας, ενώ τα χρόνια προϋπηρεσίας φάνηκε να επηρεάζουν στο αν οι συμμετέχοντες εργάζονται σε δομή που ζητάει κάποιου είδους ταυτοποίηση για την είσοδο στο ηλεκτρονικό σύστημα. Μεταξύ των διάφορων μεταβλητών για τους τύπους των δεδομένων που πρέπει να τηρούνται χειρόγραφα είναι μέτριες, ενώ και η συσχέτιση μεταξύ της επιλογής "κανένα" ως τύπος δεδομένων που πρέπει να τηρείται χειρόγραφα και της γενικής ερώτησης για το αν θα πρέπει να τηρούνται χειρόγραφα δεδομένα είναι μέτρια ενώ θα αναμενόταν πολύ υψηλότερη συσχέτιση.

Συνολικά στις αναλύσεις επαγωγικής στατιστικής φαίνεται ότι η επιρροή των δημογραφικών στοιχείων στις ειδικές ερωτήσεις του ερωτηματολογίου ήταν σχετικά

μικρή. Κάποια επιρροή φάνηκε να έχουν τα χρόνια προϋπηρεσίας και ο τύπος του επαγγελματικού πλαισίου. Παρόλα αυτά το γεγονός αυτό δε μειώνει την αξία της παρούσης έρευνας. Εξάλλου σύμφωνα με το φιλόσοφο της επιστήμης Καρλ Πόπερ ο στόχος της επιστήμης είναι η διάψευση.

3.5. Περιορισμοί της έρευνας, προτάσεις για μελλοντική έρευνα

Η παρούσα έρευνα έχει τους περιορισμούς της. Είναι μικρός ο αριθμός συμμετεχόντων, ενώ είναι σύντομος ο χρόνος που έτρεξε. Δεν υπήρχαν συμμετέχοντες από όλα τα μέρη της Ελλάδος και ήταν ελάχιστοι οι συμμετέχοντες από τις 2 χώρες του εξωτερικού. Επίσης το δείγμα λήφθηκε με βάση τη θέληση των συμμετεχόντων. Κατά συνέπεια δε μπορεί να υποστηριχθεί ότι το δείγμα είναι αντιπροσωπευτικό ούτε της Ελλάδος ούτε των υπόλοιπων χωρών που συμμετείχαν [για παράδειγμα οι γυναίκες αντιπροσωπεύουν το 70% του δείγματός μας και οι άντρες το 30% όταν στην Ελλάδα τα ποσοστά των 2 φύλων ανέρχονται στο 50%].

Η έρευνα λόγω της θεματικής της έπρεπε να επιλέξει το κοινό το οποίο θα απευθυνθεί. Εφόσον ο πληθυσμός στόχος επιλέχθηκε να είναι οι εργαζόμενοι στους χώρους υγείας (με υγειονομικές και διοικητικές ειδικότητες) και όχι επιστήμονες της επιστήμης της πληροφορικής οι τεχνικές ερωτήσεις περιορίστηκαν στο ελάχιστο.

Θα μπορούσαν να μελετηθούν περαιτέρω τα ζητήματα που σχετίζονται με την υγεία και την ασφάλεια των σχετικών πληροφοριακών συστημάτων με τη χρήση εστιασμένων ερωτηματολογίων (σε μεγάλα και αντιπροσωπευτικά δείγματα) σε διακριτές ομάδες επαγγελματιών όπως οι νομικοί, οι έχοντες υγειονομικές ειδικότητες, οι διοικητικοί υπάλληλοι και οι επιστήμονες της πληροφορικής προκειμένου να φανεί αν η νομοθεσία της Ελλάδος, της ΕΕ καθώς και χωρών όπως ο Καναδάς και η Γερμανία κινούνται στη σωστή κατεύθυνση, καθώς για τη νομοθεσία των ευαίσθητων ζητημάτων όπως είναι το απόρρητο των υγειονομικών πληροφοριών και η ασφάλεια των ηλεκτρονικών δεδομένων, καλό είναι να υπάρχει ευρεία συναίνεση μεταξύ όλων των εμπλεκόμενων φορέων.

Η εμβριθής έρευνα σε σχέση με τους προσφορότερους τρόπους διαχείρισης και διαφύλαξης των πληροφοριών που σχετίζονται με τις υπηρεσίες υγείας θα βοηθούσε πολλές ειδικότητες που σχετίζονται άμεσα ή έμμεσα με το μεγάλο κλάδο των υπηρεσιών υγείας να παρέχει όσο το δυνατόν καλύτερες και φθηνότερες υπηρεσίες σε ένα

κατάλληλο νομικό περιβάλλον, ευνοώντας το κοινωνικό σύνολο και οδηγώντας σε μια πιο ορθολογική κατανομή των οικονομικών πόρων των ασφαλιστικών ταμείων διαφόρων κρατών.

ΠΗΓΕΣ

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. *Procedia Computer Science*, *113*, 73-80.

Andreu-Perez, J., Leff, D. R., Ip, H. M., & Yang, G. Z. (2015). From wearable sensors to smart implants-–toward pervasive and personalized healthcare. *IEEE Transactions on Biomedical Engineering*, *62*(12), 2750-2762.

Andreu-Perez, J., Poon, C. C., Merrifield, R. D., Wong, S. T., & Yang, G. Z. (2015). Big data for health. *IEEE journal of biomedical and health informatics*, *19*(4), 1193-1208.

Apple (2020) https://www.apple.com/gr/researchkit/

Archana, R. A., Hegadi, R. S., & Manjunath, T. N. (2018). A Study on Big Data Privacy Protection Models using Data Masking Methods. International Journal of Electrical and Computer Engineering, 8(5), 3976.

Ashton K. (2009), *«That 'Internet of Things' thing»*, RFiD Journal

Assembly, U. G. (1948). Universal declaration of human rights. *UN General Assembly*, *302*(2).

Assembly, U. G. (1966). International covenant on economic, social and cultural rights. *United Nations, Treaty Series*, *993*(3), 2009-2057.

Attorney General (2014) https://ag.ny.gov/press-release/2014/ag-schneiderman-applauds-success-new-yorks-innovative-program-prevent

Bates, D. W., Saria, S., Ohno-Machado, L., Shah, A., & Escobar, G. (2014). Big data in health care: using analytics to identify and manage high-risk and high-cost patients. *Health Affairs*, *33*(7), 1123-1131.

Behjati, S., & Tarpey, P. S. (2013). What is next generation sequencing?. *Archives of Disease in Childhood-Education and Practice*, *98*(6), 236-238.

Bertino, E., & Ferrari, E. (2018). Big data security and privacy. In *A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years* (pp. 425-439). Springer, Cham.

Burris, J. F., & Puglisi, J. T. (2018). Impact of federal regulatory changes on clinical pharmacology and drug development: the Common Rule and the 21st Century Cures Act. *The Journal of Clinical Pharmacology*, *58*(3), 281-285.

Butler, O. (2018). Obligations imposed on private parties by the GDPR and UK Data Protection Law: Blurring the public-private divide. *European Public Law, 24*(3).

Cancer Genome Atlas Network. (2012). Comprehensive molecular portraits of human breast tumours. Nature, 490(7418), 61.

Cars, T., Wettermark, B., Malmström, R. E., Ekeving, G., Vikström, B., Bergman, U., ... & Gustafsson, L. L. (2013). Extraction of electronic health record data in a hospital setting: comparison of automatic and semi-automatic methods using anti-TNF therapy as model. *Basic & clinical pharmacology & toxicology*, *112*(6), 392-400.

Celesti, F., Celesti, A., Carnevale, L., Galletta, A., Campo, S., Romano, A., ... & Villari, M. (2017, July). Big data analytics in genomics: The point on Deep Learning solutions. In *2017 IEEE Symposium on Computers and Communications (ISCC)* (pp. 306-309). IEEE.

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. Mobile networks and applications, 19(2), 171-209.

CIHI (2020) https://www.cihi.ca/en/about-cihi/privacy-and-security

Colleaga (2020) https://www.colleaga.org/article/healthcare-privacy-legislation-canada

Commission E. The EU Data Protection Reform and Big Data: Factsheet 2016 https://publications.europa.eu/en/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1 (Accessed July 2019).

Cottle, M., Hoover, W., Kanwal, S., Kohn, M., Strome, T., & Treister, N. (2013). Transforming Health Care Through Big Data Strategies for leveraging big data in the health care industry. *Institute for Health Technology Transformation, http://ihealthtran. com/big-data-in-healthcare*.

Council for International Organizations of Medical Sciences (CIOMS): International ethical guidelines for health-related research involving humans. 2016. www.cioms.ch.

Craig, T., & Ludloff, M. E. (2011). Privacy and big data: the players, regulators, and stakeholders. " O'Reilly Media, Inc.".

Cuzzocrea, A., Loia, V., & Tommasetti, A. (2017, June). Big-data-driven innovation for enterprises: innovative big value paradigms for next-generation digital ecosystems. In *Proceedings of the 7th International Conference on Web Intelligence, Mining and Semantics* (pp. 1-5).

Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: management, analysis and future prospects. *Journal of Big Data*, *6*(1), 54.

Data Protection Laws of the World. 2017 DLA Piper. [Online]. Available: http://www.dlapiperdataprotection.com

Dey, N., Hassanien, A. E., Bhatt, C., Ashour, A., & Satapathy, S. C. (Eds.). (2018). Internet of things and big data analytics toward next-generation intelligence (pp. 3-549). Berlin: Springer.

Doneda, D., & Mendes, L. S. (2014). Data protection in Brazil: new developments and current challenges. In Reloading Data Protection (pp. 3-20). Springer, Dordrecht.

DPA (2020) https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=66,121,83,229,125,127,247,242

Dwivedi, S., Kasliwal, P., & Soni, S. (2016, March). Comprehensive study of data analytics tools (RapidMiner, Weka, R tool, Knime). In 2016 Symposium on Colossal Data Analysis and Networking (CDAN) (pp. 1-8). IEEE.

EMC (2012) https://www.emc.com/leadership/digital-universe/2012iview/big-data-2020.htm

EMC (2014) https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

Eriksson, R., Werge, T., Jensen, L. J., & Brunak, S. (2014). Dose-specific adverse drug reaction identification in electronic patient records: temporal data mining in an inpatient psychiatric population. *Drug safety*, *37*(4), 237-247.

Erl, T., Khattak, W., & Buhler, P. (2016). Big data fundamentals: concepts, drivers & techniques. Prentice Hall Press.

European Law (2016) https://eur-lex.europa.eu/eli/reg/2016/679/oj

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, *1*(2011), 1-11.

Favaretto, M., De Clercq, E., Schneble, C. O., & Elger, B. S. (2020). What is your definition of Big Data? Researchers' understanding of the phenomenon of the decade. *PloS one*, *15*(2), e0228987.

Feldman, E. A. (2012). The Genetic Information Nondiscrimination Act (GINA): public policy and medical practice in the age of personalized medicine. *Journal of general internal medicine*, *27*(6), 743-746.

Finances Online (2020) https://financesonline.com/big-data-statistics/

Friedl, M. A., Sulla-Menashe, D., Tan, B., Schneider, A., Ramankutty, N., Sibley, A., & Huang, X. (2010). MODIS Collection 5 global land cover: Algorithm refinements and characterization of new datasets. *Remote sensing of Environment*, *114*(1), 168-182.

Friedman, C., Shagina, L., Lussier, Y., & Hripcsak, G. (2004). Automated encoding of clinical documents based on natural language processing. *Journal of the American Medical Informatics Association*, *11*(5), 392-402.

Fugkeaw, S., & Sato, H. (2015, November). Privacy-preserving access control model for big data cloud. In *2015 International Computer Science and Engineering Conference (ICSEC)* (pp. 1-6). IEEE.

Garrie, D., & Byhovsky, I. (2016). Privacy and Data Protection in Russia. *JL & Cyber Warfare*, *5*, 235.

Geng, D., Zhang, C., Xia, C., Xia, X., Liu, Q., & Fu, X. (2019). Big data-based improved data acquisition and storage system for designing industrial data platform. *IEEE Access*, *7*, 44574-44582.

Gesetze (2020) https://www.gesetze-im-internet.de/englisch_bdsg/

Ginsberg J, Mohebbi MH, Patel RS, Brammer L, Smolinski MS, Brilliant L (2008) Detecting influenza epidemics using search engine query data. Nature 457(7232):1012–1014

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703-705.

Gostin, L. O., Halabi, S. F., & Wilson, K. (2018). Health data and privacy in the digital era. *Jama*, *320*(3), 233-234.

Greenleaf, G. (2011). Promises and illusions of data protection in Indian law. *International Data Privacy Law*, *1*(1), 47-69.

Hansen, T. R., Eklund, J. M., Sprinkle, J., Bajcsy, R., & Sastry, S. (2005, November). Using smart sensors and a camera phone to detect and verify the fall of elderly persons. In *European Medicine, Biology and Engineering Conference* (Vol. 20, No. 25, p. 2486).

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information systems*, *47*, 98-115.

HHS (2020) https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Hill, K. (2012). How target figured out a teen girl was pregnant before her father did. *Forbes, Inc*.

HIS (2017) https://global.ihs.com/doc_detail.cfm?document_name=JIS%20Q%2015001&item_s_key=00314502

ICLG (2020) https://iclg.com/practice-areas/data-protection-laws-and-regulations/germany

ICLG (2020) https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan

ICLG (2020) https://iclg.com/practice-areas/digital-health-laws-and-regulations/germany

Intel (2020) https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

IPC (2015) https://www.ipc.on.ca/wp-content/uploads/2015/11/phipa-faq.pdf

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. *IEEE access*, *3*, 678-708.

Jaffe, M. G., Lee, G. A., Young, J. D., Sidney, S., & Go, A. S. (2013). Improved blood pressure control associated with a large-scale hypertension program. *Jama*, *310*(7), 699-705.

Japanese Agency (2019) https://www.amed.go.jp/en/program/list/05/01/018.html

Jensen, M. (2013, June). Challenges of privacy protection in big data analytics. In *2013 IEEE International Congress on Big Data* (pp. 235-238). IEEE.

Joly, Y., Feze, I. N., Song, L., & Knoppers, B. M. (2017). Comparative approaches to genetic discrimination: chasing shadows?. Trends in Genetics, 33(5), 299-302.

Kitchin, R., & McArdle, G. (2016). What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets. *Big Data & Society*, *3*(1), 2053951716631130.

Kleine, J. (2018). General Data Protection Regulation and its effects on healthcare in the Netherlands and Germany (Bachelor's thesis, University of Twente).

Knoppers, B. M. (2014). Framework for responsible sharing of genomic and health-related data. *The HUGO journal*, *8*(1), 3.

Knoppers, B. M., & Thorogood, A. M. (2017). Ethics and big data in health. *Current Opinion in Systems Biology*, *4*, 53-57.

Knoppers, B. M., Harris, J. R., Tassé, A. M., Budin-Ljøsne, I., Kaye, J., Deschênes, M., & Ma'n, H. Z. (2011). Towards a data sharing Code of Conduct for international genomic research. *Genome Medicine*, *3*(7), 46.

KNuggets(2012) What analytics data mining, big data software you used in the past 12 months for a real project? http://www.kdnuggets. com/polls/2012/analytics-data-mining-big-data-software.html

Ko, S. Y., Jeon, K., & Morales, R. (2011). The HybrEx Model for Confidentiality and Privacy in Cloud Computing. *HotCloud*, *11*, 8-8.

Kovats, R. S., & Hajat, S. (2008). Heat stress and public health: a critical review. *Annu. Rev. Public Health*, *29*, 41-55.

Laney, D. (2001). 3-d data management: Controlling data volume, velocity and variety," META Group, Research Note, February 2001.

Laws Lois (2020) https://laws-lois.justice.gc.ca/eng/acts/P-21/FullText.html

Lawspot (2005) https://www.lawspot.gr/nomikes-plirofories/nomothesia/nomos-3418-2005

Lawspot (2020) https://www.lawspot.gr/nomika-nea/prosopika-dedomena-kai-koronoios-mporoyn-ta-nosokomeia-na-hrisimopoioyn-kameres-se

Li, N., Li, T., & Venkatasubramanian, S. (2007, April). t-closeness: Privacy beyond k-anonymity and l-diversity. In 2007 IEEE 23rd International Conference on Data Engineering (pp. 106-115). IEEE.

Lupton D. The thirteen Ps of big data 2015 https://simplysociology.wordpress.com/2015/05/11/the-thirteen-ps-of-big-data/ (Accessed, August 2019).

Lyko, K., Nitzschke, M., & Ngomo, A. C. N. (2016). Big data acquisition. In New Horizons for a Data-Driven Economy (pp. 39-61). Springer, Cham.

Makulilo, A. B. (2016). Data Protection in North Africa: Tunisia and Morocco. In *African Data Privacy Laws* (pp. 27-44). Springer, Cham.

Manyika J, McKinsey Global Institute, Chui M, Brown B, Bughin J, Dobbs R, Roxburgh C, Byers AH (2011) Big data: the next frontier for innovation, competition, and productivity. McKinsey Global Institute

Matsuo, D. (2009). Effect of Amendment to Japan's Pharmaceutical Affairs Law. *Nomura Research Institute Papers*, (149).

Miranda, M. L., Ferranti, J., Strauss, B., Neelon, B., & Califf, R. M. (2013). Geographic health information systems: a platform to support the 'triple aim'. Health affairs, 32(9), 1608-1615.

Moltchanov, S., Levy, I., Etzion, Y., Lerner, U., Broday, D. M., & Fishbain, B. (2015). On the feasibility of measuring urban air pollution by wireless distributed sensor networks. *Science of The Total Environment*, *502*, 537-547.

Moore, S. K. (2001). Unhooking medicine [wireless networking]. *IEEE Spectrum*, *38*(1), 107-108.

Mulder, T. (2019). Health apps, their privacy policies and the GDPR. European Journal of Law and Technology.

Na, L., Yang, C., Lo, C. C., Zhao, F., Fukuoka, Y., & Aswani, A. (2018). Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. JAMA network open, 1(8), e186040-e186040.

Nasi, G., Cucciniello, M., & Guerrazzi, C. (2015). The role of mobile technologies in health care processes: the case of cancer supportive care. *Journal of medical Internet research*, *17*(2), e26.

NIH (2014) https://archives.drugabuse.gov/news-events/news-releases/2014/07/nih-system-to-monitor-emerging-drug-trends

OCDE, O. (2015). *Health Data Governance*. OECD Publishing.

Ontario Law (2020) https://www.ontario.ca/laws/statute/04p03

Pilloni, V. (2018). How data will transform industrial processes: Crowdsensing, crowdsourcing and big data as pillars of industry 4.0. *Future Internet*, *10*(3), 24.

Plageras, A. P., Psannis, K. E., Stergiou, C., Wang, H., & Gupta, B. B. (2018). Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings. *Future Generation Computer Systems*, *82*, 349-357.

PMDA (2020) https://www.pmda.go.jp/english/

PPC (2020)
https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

Privacy Commisioner Canada (2019) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Rashidi, P., & Mihailidis, A. (2012). A survey on ambient-assisted living tools for older adults. *IEEE journal of biomedical and health informatics*, *17*(3), 579-590.

Rehman, M. H., Liew, C. S., Abbas, A., Jayaraman, P. P., Wah, T. Y., & Khan, S. U. (2016). Big data reduction methods: a survey. *Data Science and Engineering*, *1*(4), 265-284.

Reisman, M. (2017). EHRs: the challenge of making electronic data usable and interoperable. Pharmacy and Therapeutics, 42(9), 572.

Rosenbaum, S. (2016). Law and the Public's Health. *Public Health Reports*, *131*(2), 378.

Schmit, C. D., Wetter, S. A., & Kash, B. A. (2018). Falling short: how state laws can address health information exchange barriers and enablers. Journal of the American Medical Informatics Association, 25(6), 635-644.

Schnell-Inderst, P., Mayer, J., Lauterberg, J., Hunger, T., Arvandi, M., Conrads-Frank, A., ... & Siebert, U. (2015). Health technology assessment of medical devices: what is different? An overview of three European projects. *Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen*, *109*(4-5), 309-318.

Sedayao, J., Bhardwaj, R., & Gorade, N. (2014, June). Making big data, privacy, and anonymization work together in the enterprise: experiences and issues. In 2014 IEEE International Congress on Big Data (pp. 601-607). IEEE.

Shameer, K., Badgeley, M. A., Miotto, R., Glicksberg, B. S., Morgan, J. W., & Dudley, J. T. (2017). Translational bioinformatics in the era of real-time biomedical, health care and wellness data streams. *Briefings in bioinformatics*, *18*(1), 105-124.

SITN (2019) http://sitn.hms.harvard.edu/flash/2019/health-data-privacy/

Social Media Today (2018) https://www.socialmediatoday.com/news/how-much-data-is-generated-every-minute-infographic-1/525692/

Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy & efficiency of sustainable cloud computing for big data & IoT. Sustainable Computing: Informatics and Systems, 19, 174-184.

Sun, J., McNaughton, C. D., Zhang, P., Perer, A., Gkoulalas-Divanis, A., Denny, J. C., ... & Malin, B. A. (2014). Predicting changes in hypertension control using electronic health records from a chronic disease management program. *Journal of the American Medical Informatics Association*, *21*(2), 337-344.

Sundmaeker H., Guillemin P., Friess P., Woelffl. S. (2010), «*Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things*», CERP

Toshniwal, R., Dastidar, K. G., & Nath, A. (2015). Big data security issues and challenges. International Journal of Innovative Research in Advanced Engineering (IJIRAE), 2(2).

Traça, J. L., & Embry, B. (2012). The Angolan Data Protection Act: first impressions. International Data Privacy Law, 2(1), 40.

Tsuji, Y. (2017). Medical Privacy Issues in Ageing Japan. *Australian Journal of Asian Law*, *18*(1).

Uddin, M. F., & Gupta, N. (2014, April). Seven V's of Big Data understanding Big Data to extract value. In *Proceedings of the 2014 zone 1 conference of the American Society for Engineering Education* (pp. 1-5). IEEE.

Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing.

Wagner, J. K., Mozersky, J. T., & Pyeritz, R. E. (2014). "Use it or lose it" as an alternative approach to protect genetic privacy in personalized medicine. *Urologic oncology*, *32*(2), 198.

Wang, H., Liu, B., Zhang, Y., Jiang, F., Ren, Y., Yin, L., ... & Fan, W. (2020). Estimation of genome size using k-mer frequencies from corrected long reads. *arXiv preprint arXiv:2003.11817*.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

Wood, D. P. (2013). Re: Genome Sequencing Identifies a Basis for Everolimus Sensitivity. *The Journal of urology*.

Xu, H. (2020). Big data challenges in genomics. In Handbook of Statistics (Vol. 43, pp. 337-348). Elsevier.

Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13-53.

Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In *2010 IEEE 3rd International Conference on cloud Computing* (pp. 268-275). IEEE.

Zheng, Y. L., Ding, X. R., Poon, C. C. Y., Lo, B. P. L., Zhang, H., Zhou, X. L., ... & Zhang, Y. T. (2014). Unobtrusive sensing and wearable devices for health informatics. *IEEE Transactions on Biomedical Engineering*, *61*(5), 1538-1554.

Αλουγδέλη, Μ. (2016). Ηλεκτρονικός φάκελος ασθενούς.

Βουλη (2020) https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-9a/

Ναυτεμπορική (2019) https://m.naftemporiki.gr/story/1468186/i-proklisi-ton-big-data-stin-ugeia

Παναγοπούλου – Κουνατζή Φ. 2015.«ΧΟΡΗΓΗΣΗ ΔΕΔΟΜΕΝΩΝ ΥΓΕΙΑΣ ΜΕ ΑΔΕΙΑ ΤΗΣ ΑΡΧΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΑΠΔΠΧ: ΜΙΑ ΘΕΣΜΙΚΗ ΑΠΟΤΙΜΗΣΗ» Εφημερίδα Διοικητικού Δικαίου, τεύχος 6