Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Εφαρμοσμένη Πληροφορική της Υγείας και Τηλεϊατρική

Μεταπτυχιακή Διατριβή

Ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR – General Data Protection Regulation) στο χώρο της υγείας: Διερεύνηση και αξιολόγηση του επιπέδου ενσωμάτωσης του κανονισμού στους οργανισμούς υγείας στην Κύπρο.

Ανδρέας Χατζηπετρής

Επιβλέπων Καθηγητής: Χαράλαμπος Μπαλής

Απρίλιος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Εφαρμοσμένη Πληροφορική της Υγείας και Τηλεϊατρική

Μεταπτυχιακή Διατριβή

Ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR – General Data Protection Regulation) στο χώρο της υγείας: Διερεύνηση και αξιολόγηση του επιπέδου ενσωμάτωσης του κανονισμού στους οργανισμούς υγείας στην Κύπρο.

Ανδρέας Χατζηπετρής

Επιβλέπων Καθηγητής: Χαράλαμπος Μπαλής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Εφαρμοσμένη πληροφορική στην υγεία και Τηλεϊατρική από τη Σχολή θετικών και εφαρμοσμένων επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Απρίλιος 2020

Περίληψη

Ο στόχος της διατριβής είναι να συνδεθούν οι κανονισμοί του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων στον τομέα της υγείας και η ανταπόκριση των οργανωμένων ομάδων και υπεύθυνων φορέων στην Κύπρο για την εφαρμογή των νέων κανονισμών. Επίσης στόχος είναι να προσδιορίσει τον αντίκτυπο, τα πλεονεκτήματα και τις αδυναμίες των εκτελεστικών κανονισμών και να προταθούν πιθανές λύσεις και ενέργειες. Αυτά τα μέτρα μπορούν να βοηθήσουν στην πιο ομαλή έγκριση κανονισμών χωρίς να μειωθεί το επίπεδο υγειονομικής περίθαλψης. Για τους σκοπούς αυτούς, πραγματοποιήθηκε ένα online ερωτηματολόγιο, το οποίο εστάλη μέσω email σε διάφορα νοσοκομεία, κλινικές και άλλους οργανισμούς υγείας της Κύπρου.

Τα αποτελέσματα αυτής της μελέτης έδειξαν ότι οι υπάλληλοι στους οργανισμούς υγείας χρειάζονται περισσότερες πληροφορίες σχετικά με την πολιτική απορρήτου και ότι είναι πολύ σημαντικός ο νέος κανονισμός προστασίας προσωπικών δεδομένων στον τομέα της υγείας. Επιπλέον, οι οργανισμοί έχουν κάνει ελάχιστες αλλαγές στις διαδικασίες και στα έντυπα για την ενημέρωση του προσωπικού σχετικά με τον καινούργιο κανονισμό του 2018.

Επιπρόσθετα, οι συμμετέχοντες τόνισαν πολλά προβλήματα στην εφαρμογή του νέου κανονισμού στους οργανισμούς όπου δουλεύουν. Για παράδειγμα, ένα μεγάλο ποσοστό απάτησε δεν εφαρμόζεται καθόλου ικανοποιητικά ο κανονισμός στον οργανισμό όπου δουλεύουν. Ένα άλλο μεγάλο πρόβλημα είναι ότι σχεδόν οι μισοί συμμετέχοντες δήλωσαν ότι δεν είχαν ενημέρωση για τον νέο κανονισμό από τη διοίκηση του νοσοκομείου ή/και κλινικής.

Τέλος, η έρευνα έδειξε ότι ένα μεγάλο ποσοστό των εργαζομένων στους οργανισμούς υγείας δε γνωρίζουν καθόλου τα δικαιώματα τους που απορρέουν από τον Κανονισμό, ενώ ένα άλλο μεγάλο ποσοστό γνωρίζει μερικώς τα δικαιώματα τους.

Summary

The dissertation aims to link the regulations of the General Regulation of Personal Data Protection in the field of health with the response of organized groups and responsible bodies in Cyprus with the implementation of the new regulations as well as to determine the impact, strengths, and weaknesses of enforcement regulations and suggest possible solutions and actions. These measures and measures can help to smoothly adopt regulations without reducing the level of healthcare. For these purposes, an online questionnaire was conducted, which was sent via email to various hospitals, clinics, and other health organizations in Cyprus.

The results of this study showed that employees in health organizations need more information about privacy policy and that the new regulation on personal data protection in the field of health is very important. Besides, the agencies have made minimal changes to the procedures and forms for informing staff about the new 2018 regulation.

Also, the participants highlighted many problems in the implementation of the new regulation in the organizations where they work. For example, a large percentage of cheats do not apply the regulation satisfactorily to the organization where they work. Another big problem is that almost half of the participants stated that they were not informed about the new regulation by the administration of the hospital and/or clinic.

Finally, research has shown that a large percentage of employees in health organizations are not at all aware of their rights under the Regulation while another large percentage is partially aware of their rights. The dissertation aims to link the regulations of the General Regulation of Personal Data Protection in the field of health with the response of organized groups and responsible bodies in Cyprus with the implementation of the new regulations as well as to determine the impact, strengths, and weaknesses of enforcement regulations and suggest possible solutions and actions. These measures and measures can help to smoothly adopt regulations without reducing the level of healthcare. For these purposes, an online questionnaire was conducted, which was sent via email to various hospitals, clinics, and other health organizations in Cyprus.

The results of this study showed that employees in health organizations need more information about privacy policy and that the new regulation on personal data protection

in the field of health is very important. Besides, the agencies have made minimal changes to the procedures and forms for informing staff about the new 2018 regulation.

Also, the participants highlighted many problems in the implementation of the new regulation in the organizations where they work. For example, a large percentage of cheats do not apply the regulation satisfactorily to the organization where they work. Another big problem is that almost half of the participants stated that they were not informed about the new regulation by the administration of the hospital and/or clinic.

Finally, research has shown that a large percentage of employees in health organizations are not at all aware of their rights under the Regulation while another large percentage is partially aware of their rights.

Λέξεις Κλειδιά / Keywords : Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ), Χώρος Υγείας, Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ), General Data Protection Regulation (GDPR), Data Protection Officer (DPO), προσωπικά δεδομένα, health information system (HIS), e-Health, data protection, blockchain, big data, regulation (EU) 2016/679, health clinics, data privacy.

Ευχαριστίες

Είμαι ευγνώμων για τη βοήθεια και την καθοδήγηση από τον Δρ. Χαράλαμπος Μπαλής καθ' όλη τη διάρκεια της διατριβής, οι συμβουλές και οι καθοδηγήσεις του ήταν οδηγός για την επίτευξη της διατριβής. Θέλω επίσης να εκφράσω τις ευχαριστίες μου σε όλους τους ανθρώπους που συμμετείχαν σε αυτήν την έρευνα και επειδή ξόδεψαν λίγο από το πολύτιμο χρόνο τους μαζί μου στη μέση των πολυάσχολων προγραμμάτων τους. Η συμμετοχή τους έκανε αυτήν την έρευνα πολύτιμη εμπειρία στο μέσω μίας δύσκολης κατάστασης που βιώνει ο πλανήτης με τη καινούργια πανδημία και τον ιό COVID-19. Ευχαριστώ επίσης τους φίλους και την οικογένεια μου που ήταν δίπλα μου και σε αυτό το ταξίδι γνώσεων.

Περιεχόμενα

Κεφάλαιο 1

1.1 Εισαγωγή

Υπάρχουν πολλοί λόγοι για τους οποίους επιλέχθηκε για μελέτη ο κανονισμός Προστασίας Προσωπικών Δεδομένων στο τομέα της Υγείας. Αρχικά ο βασικότερος λόγος είναι η ενασχόληση του ερευνητή με τα προσωπικά δεδομένα στην παρούσα εργασία του και η καθημερινή τριβή με προσωπικά δεδομένα υγείας ασθενών. Μέσα από την εμπειρία του ερευνητή με το GDPR του δόθηκε η ευκαιρία να οδηγηθεί στο συμπέρασμα ότι υπάρχει έλλειψη πληροφοριών σχετικά με την εφαρμογή του κανονισμού, καθώς και στο επίπεδο συμμόρφωσης του κανονισμού στην ΕΕ αλλά κυρίως στην Κύπρο. Επίσης ένας άλλος βασικός λόγος είναι η κατανόηση της συσχέτισης της υγείας με τα προσωπικά δεδομένα και η αντίληψη του πόσο σημαντική είναι η διασφάλιση των προσωπικών δεδομένων στο χώρο αυτό. Επιπρόσθετα, επιλέχθηκε αυτό το αντικείμενο μελέτης με σκοπό την εκμάθηση του κανονισμού και του σκοπού του, από τους επαγγελματίες υγείας αφού παρατηρήθηκε ότι αρκετοί επαγγελματίες υγείας δεν γνωρίζουν επαρκώς για το κανονισμό.

1.2 Σκοποί και στόχοι

Στη συγκεκριμένη μεταπτυχιακή διατριβή, ο σκοπός είναι η συσχέτιση του κανονισμού με το τομέα της υγείας και πως τα οργανωμένα σύνολα και οι υπεύθυνοι φορείς στην Κύπρο αντέδρασαν για την εφαρμογή του καινούργιου κανονισμού. Επίσης σκοπός της έρευνας είναι να προσδιορίσει τις επιπτώσεις που προήλθαν κατά την εφαρμογή του κανονισμού, τα πλεονεκτήματα, τα μειονεκτήματα και να προτείνει πιθανόν λύσεις και ενέργειες που μπορούν να βοηθήσουν για την πιο ομαλή υιοθέτηση του κανονισμού χωρίς να μειώσει το επίπεδο παροχής υγειονομικής περίθαλψης.

Στόχοι της έρευνας είναι:

- Η μελέτη και η κατανόηση του καινούργιου κανονισμού (GDPR) της ΕΕ.
- Αντίληψη για το ποια δεδομένα χαρακτηρίζονται ως προσωπικά και ποιος ο βαθμός «ευαισθησίας» κάθε δεδομένου.
- Κατανόηση των λόγων που οδήγησαν στην ανάγκη για τον Κανονισμό.
- Γνωριμία με το γενικό πλαίσιο εφαρμογής του νέου Κανονισμού – διάκριση αλλαγών.
- Να μάθουμε σε ποιο στάδιο βρίσκονται μέχρι στιγμής τα διάφορα συστήματα υγείας ως προς την εφαρμογή του Κανονισμού.

Ακόμη βασικά ερευνητικά ερωτήματα που προκύπτουν είναι:

- Ποιες ενέργειες προχώρησαν τα διάφορα γενικά συστήματα υγείας σε διάφορες χώρες της ΕΕ;
- Ποιες οι δυσκολίες που αντιμετώπισαν και αντιμετωπίζουν οι διάφορες χώρες προς την εφαρμογή του κανονισμού;
- Ποια τα προβλήματα που προέκυψαν και δεν αντιμετωπίστηκαν, είτε αφορά οικονομικό κόστος, είτε το εργασιακό περιβάλλον από αντιδράσεις των επαγγελματιών υγείας ή δυσκολίες των επαγγελματιών υγείας;

1.3 Προσωπικά Δεδομένα

Η έννοια των «προσωπικών δεδομένων» αναλύεται σε δύο υποσυστήματα, συγκεκριμένα την πληροφορία και τα φυσικά πρόσωπα που είναι άρρηκτα συνδεδεμένα, αλληλοεπιδρούν μεταξύ τους και αποτελούν εννοιολογικά τον παραπάνω όρο. Οι πληροφορίες ορίζονται ως κάθε είδηση που αλλάζει σημαντικά τις αντιλήψεις και επηρεάζει το περιεχόμενο των αποφάσεων των παραληπτών της. Σύμφωνα με τις διατάξεις της Υπηρεσίας Προστασίας Προσωπικών Δεδομένων (APDP), τα προσωπικά δεδομένα περιλαμβάνουν οποιεσδήποτε πληροφορίες που μπορούν να χαρακτηρίσουν και να προσδιορίσουν φυσικά πρόσωπα. Το φυσικό πρόσωπο νοείται ως "υποκείμενο δεδομένων" (ν. 2472/1997, άρθρο 2, εδ. α '), ποια είναι η πηγή του, ποιες πληροφορίες παρέχει στον κάτοχο και την προσωπικότητά του, όπως όνομα, διεύθυνση, Τηλεφωνικές κλήσεις, ενδιαφέροντα, φωτογραφίες και προσωπικές απόψεις. Ορισμένες προσωπικές πληροφορίες σχετίζονται με ιδιαίτερα ευαίσθητες πτυχές του προσωπικού απορρήτου, όπως θρησκεία, πολιτικές πεποιθήσεις, κατάσταση υγείας ή ερωτική ζωή. (Παναγοπούλου – Κουτνατζή, 2012).

Προσωπικά δεδομένα ορίζεται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Το ταυτοποιήσιμο φυσικό πρόσωπο, είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, αριθμός ταυτότητας, δεδομένα θέσης, επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου. Συνεπώς, “Προσωπικά δεδομένα”, είναι κάθε πληροφορία που αναφέρεται σε ένα άτομο ή το περιγράφει. Όπως στοιχεία αναγνώρισης που μπορεί να είναι ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση, φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες, επιγραμμικά στοιχεία (π.χ. διεύθυνση IP, GPS). Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται «υποκείμενο των δεδομένων».

Άρα τα προσωπικά δεδομένα είναι κάθε πληροφορία που σχετίζεται με ένα ταυτοποιημένο ή αναγνωρίσιμο ζωντανό άτομο. Επίσης διαφορετικά στοιχεία που συλλέγονται μαζί μπορούν να οδηγήσουν στον προσδιορισμό ενός συγκεκριμένου ατόμου και αποτελούν προσωπικά δεδομένα. Προσωπικά δεδομένα που έχουν

αποκρυπτογραφηθεί ή μετατραπεί σε ψευδώνυμο, αλλά μπορούν να χρησιμοποιηθούν για την ταυτοποίηση ενός ατόμου παραμένουν προσωπικά δεδομένα και εμπίπτουν στο πεδίο εφαρμογής του GDPR. Αντιθέτως προσωπικά δεδομένα που έχουν καταστεί ανώνυμα με τέτοιο τρόπο ώστε το άτομο να μην είναι ή να αναγνωρίζεται πλέον, δεν θεωρούνται πλέον προσωπικά δεδομένα. Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμοποίηση πρέπει να είναι μη αναστρέψιμη. Το GDPR προστατεύει τα προσωπικά δεδομένα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία αυτών. Είναι τεχνολογικά ουδέτερο και ισχύει τόσο για την αυτοματοποιημένη όσο και για τη μη αυτόματη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα είναι οργανωμένα σύμφωνα με προκαθορισμένα κριτήρια (για παράδειγμα αλφαβητική σειρά). Επίσης, δεν έχει σημασία πώς αποθηκεύονται τα δεδομένα, δηλαδή, είτε σε ένα σύστημα πληροφορικής, ή μέσω παρακολούθησης βίντεο ή σε χαρτί. Σε όλες τις περιπτώσεις, τα προσωπικά δεδομένα υπόκεινται στις απαιτήσεις προστασίας που ορίζονται στον GDPR.

1.3.1 Ειδικές κατηγορίες προσωπικών δεδομένων

Μια άλλη προσέγγιση των «προσωπικών δεδομένων» διατυπώνεται στην Οδηγία 95/46/ΕΚ ως: «κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή είναι δυνατόν να εξακριβωθεί άμεσα ή έμμεσα ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική». Αναγνωρίζεται ότι το όνομα είναι το πιο κοινό αναγνωριστικό για ένα άτομο, αλλά το όνομα μπορεί να είναι ισοδύναμο με άλλα στοιχεία, όπως ο αριθμός μητρώου της κοινωνικής ασφάλισης (Α.Μ.Κ.Α.), ο αριθμός του δελτίου αστυνομικής ταυτότητας, ο αριθμός φορολογικού μητρώου κτλ. Επιπλέον, οι πληροφορίες που προσδιορίζουν το άτομο και οι νομικές πληροφορίες που αποδίδονται ή επιλέγονται από το άτομα μπορεί να είναι ταυτότητα ή κωδικός πρόσβασης.

Τα λεγόμενα «απλά» προσωπικά δεδομένα είναι το εξής: το ονοματεπώνυμο, η κατοικία, το επάγγελμα, το μορφωτικό επίπεδο, οι καταναλωτικές συνήθειες, η ταξιδιωτική δραστηριότητα, η οικογενειακή και περιουσιακή κατάσταση, ο μισθός και οι τραπεζικοί λογαριασμοί (Βλ. εικόνα 1). Αυτές οι «αβλαβείς» πληροφορίες, η δημοσιοποίηση των οποίων δεν αντιμετωπίζεται, συνήθως, με ανησυχία από το άτομο αντιπαραβάλλονται με εκείνες που συνθέτουν τον «σκληρό πυρήνα» της ιδιωτικής του ζωής, τα «ευαίσθητα» προσωπικά δεδομένα. Είναι δεδομένα που έχουν ιδιαίτερη σημασία για τον σχηματισμό της εικόνας της προσωπικότητας του, πληροφορίες τις οποίες θεωρεί ιδιωτικές και για τον λόγο αυτό επιθυμεί να απαγορεύσει ή να περιορίσει τη συλλογή, τη χρήση και τη διάδοση τους (ν. 2472/1997. Αρ 2, εδ. β') .

Σε κάθε χώρα, η έννοια της ιδιωτικής ζωής είναι διαφορετική. Στη χώρα μας, τα «ευαίσθητα» προσωπικά δεδομένα σχετίζονται με: φυλή ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, ένταξη στην ένωση, κατάσταση υγείας, ερωτική ζωή, ποινικές διώξεις ή ποινικά αρχεία, ενώσεις προσώπων που

εμπλέκονται σε ευαίσθητα προσωπικά δεδομένα, δεδομένα σχετικά με παραλήπτες και δότες ανθρώπινων ιστών και οργάνων και γενικά δεδομένα.

Στην πράξη, ο διαχωρισμός των προσωπικών δεδομένων σε απλά και ευαίσθητα σχετίζεται με τη διαδικασία συλλογής και επεξεργασίας προσωπικών δεδομένων, διότι αρκεί η νόμιμη επεξεργασία απλών δεδομένων, η προφορική συγκατάθεση του ατόμου και η κοινοποίηση στην αρμόδια Αρχή (ΑΠΔΠΧ). Αντιθέτως, για ευαίσθητα δεδομένα, έχει εισαχθεί μια γενική απαγόρευση της επεξεργασίας τους. Σε ειδικές περιπτώσεις, αφού λάβουν άδεια από την ΑΠΔΧ, μπορούν να συλλεχθούν και να υποβληθούν σε επεξεργασία και να διατηρηθούν τα σχετικά έγγραφα (Αλεξανδροπούλου - Αιγυπτιάδου, 2007).

Για τη λήψη άδειας από την ΑΠΔΧ, θα πρέπει να συντρέχουν συγκεκριμένοι λόγοι (αρ. 7 ν.2472/1997), όπως:

- Η γραπτή συγκατάθεση του υποκείμενου των δεδομένων.
- Η προστασία των ζωτικών συμφερόντων των ατόμων είναι μια πράξη που δεν μπορεί να λάβει τη συγκατάθεσή τους φυσικά ή νομικά.
- Η αναγκαιότητα αναγνώρισης, άσκησης ή υπεράσπισης δικαιώματος ενώπιων δικαστηρίου ή πειθαρχικού οργάνου (αρ22 ν.3471/2006).
- Η ιατρική πρόληψη, διάγνωση, περίθαλψη ή διαχείριση υπηρεσιών υγείας (αρ,34 ν.2915/2001).
- Η εθνική ασφάλεια, η διακρίβωση εγκλημάτων ποινικών καταδικών ή τη λήψη μέτρων ασφάλειας.
- Η προστασία της δημόσιας υγείας, η άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών (αρ.34 ν. 2915/2001).
- Η πραγματοποίηση επιστημονικής έρευνας ενώ προβλέπεται και η διενέργεια προληπτικού ελέγχου τήρησης των δεδομένων αυτών (ν. 2472/1997).

Σε όλους τους τομείς της ανθρώπινης ζωής, η τεχνολογία αλλάζει κάθε μέρα, η πληροφορία μεταδίδεται ανά το παγκόσμιο και το διαδίκτυο ξαφνικά εισβάλλει στις προσωπικές ζωές των ατόμων ανεξέλεγκτα. Αυτό που ακολουθεί είναι, η συρρίκνωση της βασικής ελευθερίας του ατόμου και της κοινωνικής και πολιτικής ελευθερίας του ατόμου. Αυτό έχει ως αποτέλεσμα να κάνουν περισσότερο από ποτέ επιτακτική την ανάγκη προστασίας των προσωπικών δεδομένων και ενιαίας αντιμετώπισής απ' όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης. Ο Γενικός Κανονισμός 2016/679/ΕΕ σε σχέση με την κοινοτική Οδηγία 95/46/ΕΚ προσέθεσε, ως νέες ειδικές κατηγορίες δεδομένων τα γενετικά δεδομένα, τα βιομετρικά δεδομένα (π.χ. δακτυλοσκοπικά δεδομένα, εικόνες) και δεδομένα που σχετίζονται με τον γενετήσιο προσανατολισμό. Πληροφορίες οι οποίες συλλαμβάνουν την επεξεργασία και την εξέλιξη των δημοφιλών κοινωνικών εννοιών, ευαίσθητες ή ειδικές κατηγορίες προσωπικών δεδομένων που σχετίζονται με τον πυρήνα του απορρήτου των ανθρώπων στο παρόν ή στο παρελθόν ή στο μέλλον.

Η μη τήρηση των κανόνων του ΓΚΠΔ μπορεί να οδηγήσει σε σημαντικά πρόστιμα που μπορούν να φθάσουν μέχρι τα 20 εκατομμύρια ευρώ ή το 4% του συνολικού κύκλου εργασιών της επιχείρησης για ορισμένες παραβάσεις. Η Αρχή Προστασίας Δεδομένων μπορεί επίσης να λάβει άλλα διορθωτικά μέτρα, όπως να διατάξει μια επιχείρηση να σταματήσει την επεξεργασία προσωπικών δεδομένων.

Εικόνα 1. Τι είναι τα προσωπικά δεδομένα.

1.3.2 Ιστορική Αναδρομή Προσωπικών δεδομένων

Η προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων είναι δύο αλληλένδετοι όροι που χρησιμοποιούνται συχνά ενιαία, αλλά στην πραγματικότητα αποτελούν δύο διακριτές και διαφορετικές έννοιες. Η ιδέα της ιδιωτικής ζωής στην Ευρώπη προέρχεται από έννοιες όπως η ανθρώπινη αξιοπρέπεια και το κράτος δικαίου. Οι αντιλήψεις για την ιδιωτικότητα έχουν αρχίσει να αναπτύσσονται μετά τις εμπειρίες του φασισμού στον Β' Παγκόσμιο Πόλεμο και του κομμουνισμού κατά τη μεταπολεμική περίοδο. Στο ευρωπαϊκό δίκαιο υπάρχει διάκριση μεταξύ «Προστασία της ιδιωτικής ζωής» και «προστασία δεδομένων» που καθορίζει αυτές τις δύο έννοιες ως στενά συνδεδεμένα και συχνά αλληλεπικαλύπτονται, αλλά όχι τόσο συνώνυμα. Το απόρρητο αναφέρεται γενικά στην προστασία του «προσωπικού χώρου» ενός ατόμου, ενώ η προστασία δεδομένων αναφέρεται σε περιορισμούς ή προϋποθέσεις για την επεξεργασία δεδομένων σχετικά με ένα αναγνωρίσιμο άτομο.

Η ιστορία των προσωπικών δεδομένων ξεκινάει πολλά χρόνια πίσω στο 1890 όπου δύο δικηγόροι των Ηνωμένων Πολιτειών, ο Samuel D. Warren και ο Louis Brandeis, γράφουν το The Right to Privacy, ένα άρθρο που υποστηρίζει το «δικαίωμα να μείνεις μόνος», χρησιμοποιώντας τη φράση ως ορισμό της ιδιωτικής ζωής. Ακολούθως το 1948 γίνεται

διακήρυξη των ανθρωπίνων δικαιωμάτων τα οποία υιοθετούνται, συμπεριλαμβανομένου του 12ου θεμελιώδους δικαιώματος, δηλαδή του δικαιώματος στην ιδιωτική ζωή. Στη συνέχεια το 1950 η ακολουθία των θεμελιωδών δικαιωμάτων της σύμβασης της ΕΕ για τα ανθρώπινα δικαιώματα τροποποιείται και εμπλουτίζεται με άρθρα. Ακολούθως το 1967 στις ΗΠΑ, τίθεται σε ισχύ ο νόμος περί ελευθερίας της πληροφόρησης (FOIA) και παρέχει σε όλους το δικαίωμα να ζητούν πρόσβαση σε έγγραφα από κρατικές υπηρεσίες, κάτι που ακολούθησαν και άλλες χώρες. Το 1980 στην ΕΕ εκδίδονται κατευθυντήριες γραμμές για την προστασία δεδομένων, που αντικατοπτρίζουν την αυξανόμενη χρήση υπολογιστών για την επεξεργασία επιχειρηματικών συναλλαγών. Ένα χρόνο αργότερα το 1981 το Συμβούλιο της Ευρώπης υιοθετεί τη σύμβαση για την Προστασία Δεδομένων (Συνθήκη 108), καθιστώντας το δικαίωμα στην ιδιωτική ζωή. Δύο χρόνια αργότερα το 1983 το Ομοσπονδιακό Συνταγματικό Δικαστήριο της Γερμανίας λαμβάνει μια θεμελιώδη απόφαση σχετικά με την απόφαση απογραφής. Η ετυμηγορία θεωρείται ορόσημο της προστασίας προσωπικών δεδομένων. Μετέπειτα το 1993 το PC Brown χρεώνεται με το αδίκημα περί χρήσης προσωπικών δεδομένων ή σκοπού διαφορετικού από αυτόν που περιγράφεται στο Μητρώο Προστασίας Δεδομένων του Ηνωμένου Βασιλείου περί προστασίας δεδομένων 1984 και η απόφαση ανατρέπεται. Το μεγαλύτερο βήμα γίνεται το 1995 όπου συντάσσετε η Ευρωπαϊκή Οδηγία για την προστασία δεδομένων. Η νέα οδηγία αντικατοπτρίζει τις τεχνολογικές εξελίξεις και εισάγει νέους όρους, μεταξύ άλλων, την επεξεργασία, τα ευαίσθητα προσωπικά δεδομένα και τη συναίνεση. Το 2002 η ΕΕ εκδίδει την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Ακολούθως το 2006 συντάσσετε η οδηγία της ΕΕ για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε σχέση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών. Αργότερα η οδηγία αυτή κηρύχθηκε άκυρη με απόφαση του Δικαστηρίου το 2014 για παραβίαση θεμελιωδών δικαιωμάτων. Το 2009 γίνεται μία αναβάθμιση και εξέλιξη των κανονισμών ηλεκτρονικών επικοινωνιών της ΕΕ ως απάντηση στις διευθύνσεις ηλεκτρονικού ταχυδρομείου και τους αριθμούς κινητής τηλεφωνίας που γίνονται πρωταρχικό μέσο στη διεξαγωγή εκστρατειών μάρκετινγκ και πωλήσεων. Ένα χρόνο αργότερα το 2010 ο διεθνής μη κερδοσκοπικός οργανισμός Wikileaks δημοσιεύει μυστικές πληροφορίες, διαρροές ειδήσεων και διαβαθμισμένα μέσα που παρέχονται από ανώνυμες πηγές. Η κίνηση αυτή προκάλεσε την ΕΕ και φανέρωσε τα κενά της οδηγίας περί προστασίας των προσωπικών δεδομένων. Το 2013 η Ευρωπαϊκή Επιτροπή εκδίδει τον κανονισμό 611/2013 σχετικά με τα μέτρα που ισχύουν για την κοινοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα βάσει της οδηγίας 2002/58 / ΕΚ. Το 2014 με απόφαση του Δικαστηρίου της ΕΕ διαπιστώνεται ότι ο ευρωπαϊκός νόμος δίνει στους ανθρώπους το δικαίωμα να ζητούν από μηχανές αναζήτησης όπως το Google να καταργήσουν αποτελέσματα για ερωτήματα που περιλαμβάνουν το όνομά τους. Η ιδέα γίνεται γνωστή ως «the right to be forgotten». Ακολούθως το 2016 μετά από 4 χρόνια συζητήσεων και διαπραγματεύσεων εγκρίνεται από το κοινοβούλιο της ΕΕ ο γενικός κανονισμός για την προστασία δεδομένων (GDPR). Ο κανονισμός αυτός λόγο των μεγάλων αλλαγών, ψηφίζεται αλλά δίνεται μία περίοδος προσαρμογής περίπου 2 χρόνια και έρχεται το 2018 όπου το GDPR εφαρμόζεται, αντικαθιστώντας τον Νόμο περί προστασίας δεδομένων.

1.4 Επεξεργασία Προσωπικών Δεδομένων

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί βασικό παράγοντα στη λήψη αποφάσεων και σχεδίων από το δημόσιο και τον ιδιωτικό τομέα σε οικονομικό, διοικητικό, πολιτικό και κοινωνικό επίπεδο. Η επεξεργασία των προσωπικών δεδομένων είναι μια πολύ ευρεία έννοια. Σύμφωνα με την Οδηγία 95/46/ΕΚ (άρθρο 2) αλλά και με το ν. 2472/1997 ως υλοποίηση της Οδηγίας, η επεξεργασία προσωπικών δεδομένων ορίζεται ως «Κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, εργασίες όπως συλλογή, καταχώρηση, οργάνωση, αποθήκευση, προσαρμογή ή τροποποίηση, ανάκτηση, αναζήτηση πληροφοριών, χρήση, ανακοίνωση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, εναρμόνιση ή συνδυασμός, καθώς και κλείδωμα, διαγραφή ή καταστροφή».
Η επεξεργασία των δεδομένων σχετίζεται με ορισμένες έννοιες όπως αυτές του υπεύθυνου, του εκτελούντα, του τρίτου και του αποδέκτη. Η έννοια του υπεύθυνου επεξεργασίας ως: «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Όταν οι στόχοι και ο τρόπος της επεξεργασίας καθορίζονται από νομοθετικές ή κανονιστικές διατάξεις, εθνικές ή κοινοτικές, ο υπεύθυνος της επεξεργασίας ή τα ειδικά κριτήρια για τον ορισμό του μπορούν να καθορίζονται από το εθνικό ή κοινοτικό δίκαιο». Ο υπεύθυνος προστασίας δεδομένων συνεργάζεται επίσης με την Αρχή Προστασίας Δεδομένων (ΑΠΔ), λειτουργώντας ως σημείο επαφής μεταξύ της ΑΠΔ και μεμονωμένων ατόμων. Ο υπεύθυνος επεξεργασίας πρέπει να διακρίνεται από το προσωπικό που επεξεργάζεται προσωπικά δεδομένα, καθώς και από τρίτους που δεν διαθέτουν καμία από τις παραπάνω ιδιότητες αλλά λειτουργεί υπό την άμεση επίβλεψη του ελεγκτή.
Το άρθρο 10 του ν. 2472/1997, αναφέρει ότι: «Η επεξεργασία των προσωπικών δεδομένων είναι απόρρητη και εκτελείται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του». Οι υπεύθυνοι επεξεργασίας, ανεξάρτητα από το εάν εξαιρείται από την υποχρέωση γνωστοποίησης και λήψης άδειας από την Αρχή Προστασίας Προσωπικών Δεδομένων, πρέπει να επιλέξει προσωπικό με επαρκείς τεχνικές γνώσεις και προσωπική ακεραιότητα για να το διατηρήσει εμπιστευτικό. Πρέπει επίσης να λάβουν κατάλληλα οργανωτικά και τεχνικά μέτρα για να διασφαλίσουν ότι το επίπεδο ασφάλειας είναι ανάλογο με τους κινδύνους που ενέχουν τα δεδομένα επεξεργασίας και τη φύση των δεδομένων επεξεργασίας. Οι κίνδυνοι και οι απειλές που αντιμετωπίζει το σύστημα πληροφοριών για την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να αξιολογούνται, από τον υπεύθυνο επεξεργασίας, μέσω ανάλυσης κινδύνου και πρέπει να λαμβάνονται κατάλληλα μέτρα ασφάλειας βάσει των αποτελεσμάτων για τη μείωση του κινδύνου σε αποδεκτό επίπεδο.

Εάν μια εταιρεία παρακολουθεί τακτικά ή συστηματικά άτομα, ή επεξεργάζεται συγκεκριμένες κατηγορίες δεδομένων και επεξεργάζεται δεδομένα ως μία από τις κύριες επιχειρηματικές της δραστηριότητες και επεξεργάζεται δεδομένα σε μεγάλη κλίμακα, πρέπει να διοριστεί υπεύθυνος προστασίας δεδομένων. Αν μια επιχείρηση επεξεργάζεται και συλλέγει δεδομένα για την υγεία ασθενών, πιθανότατα να μην χρειάζεται υπεύθυνο επεξεργασίας προσωπικών δεδομένων. Ωστόσο, αν επεξεργάζεται προσωπικά δεδομένα γενετικής και υγείας για λογαριασμό νοσοκομείου ή κλινικής, οφείλει να έχει υπεύθυνο επεξεργασίας. Ο υπεύθυνος επεξεργασίας μπορεί να προέρχεται από το προσωπικό του οργανισμού ή να είναι εξωτερικός συνεργάτης βάσει σύμβασης παροχής υπηρεσιών.
Στην περίπτωση που η επεξεργασία εκτελείται για λογαριασμό του υπευθύνου επεξεργασίας από τρίτο πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως και προβλέπει ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατόπιν εντολής του υπευθύνου επεξεργασίας και ότι οι λοιπές υποχρεώσεις του άρθρου 10 του ν. 2472/1997 βαρύνουν αναλόγως και αυτόν. Η συλλογή και επεξεργασία προσωπικών δεδομένων, απλών και ευαίσθητων απαγορεύεται, εκτός εάν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του.
Ως αποδέκτης ορίζεται κατά το άρθρο 2 στοιχείο ι' του ν. 2472/1997 ως «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμό, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως αν πρόκειται για τρίτο ή όχι».
Η απλή και ευαίσθητη επεξεργασία προσωπικών δεδομένων δεν οδηγεί πάντα σε απαράδεκτες παρεμβολές στον προσωπικό τομέα των ατόμων, αλλά μπορεί να δικαιολογηθεί από τη συμμόρφωση με ορισμένες αρχές που πρέπει να τηρεί ο υπεύθυνος επεξεργασίας. Η παράβαση των αρχών αυτών υποχρεώνει τον υπεύθυνο επεξεργασίας να καταστρέψει τα προσωπικά στοιχεία που έχουν συλλεχθεί.
Επομένως, για να θεωρηθεί νομική οποιαδήποτε επεξεργασία προσωπικών δεδομένων, πρέπει να τηρούνται οι τέσσερις αρχές επεξεργασίας, πρέπει να τηρούνται με τη συγκατάθεση του υποκειμένου των δεδομένων, διαφορετικά να εξεταστούν αν πληρούνται οι προϋποθέσεις μη συγκατάθεσης, να ενημερωθεί το υποκείμενο και να γνωστοποιηθεί η πρόθεση της συλλογής και επεξεργασίας προσωπικών δεδομένων στην Αρχή Προστασίας Προσωπικών Δεδομένων ή να ληφθεί η άδεια της Αρχής σε περίπτωση ευαίσθητων δεδομένων. Όλα τα προαναφερόμενα, αναπροσαρμόζονται σύμφωνα με τον νέο Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων.
Ο ΓΚΠΔ (Γενικός Κανονισμός Προστασίας Δεδομένων) ορίζει αυστηρούς κανόνες για την επεξεργασία δεδομένων βάσει συγκατάθεσης. Ο σκοπός αυτών των κανόνων είναι να διασφαλιστεί ότι το υποκείμενο των δεδομένων κατανοεί για τι πραγματικά έδωσε τη συγκατάθεση του. Αυτό σημαίνει ότι η συγκατάθεσή πρέπει να δίνεται ελεύθερα, συγκεκριμένα και χωρίς ασάφειες με δήλωση διατυπωμένη σε απλή και κατανοητή γλώσσα. Η συγκατάθεση πρέπει να δίνεται με καταφατική πράξη. Όταν έχει δώσει συγκατάθεση για την επεξεργασία προσωπικών δεδομένων, η εταιρεία ή ο οργανισμός μπορεί να επεξεργαστεί τα δεδομένα μόνο για τους σκοπούς για τους οποίους δόθηκε η συγκατάθεση από το υποκείμενο των δεδομένων. Πρέπει επίσης να δίνετε στο υποκείμενο των δεδομένων τη δυνατότητα να αποσύρει τη συγκατάθεσή του οποιαδήποτε στιγμή επιθυμεί χωρίς περιττή γραφειοκρατία.

Κεφάλαιο 2

2.1 Ηλεκτρονικά αρχεία υγείας

Τα αρχεία υγείας που βασίζονται σε χαρτί και χρησιμοποιούνται αυτήν την στιγμή δημιουργούν μεγάλες ποσότητες χαρτιού, με πληροφορίες και προσωπικά δεδομένα. Οι άνθρωποι ανησυχούν πολύ για τη μετάβαση από τα αρχεία υγείας χαρτιού σε ηλεκτρονικά αρχεία υγείας (EHR) σχετικά με τον όγκο τους και το χειρισμό τους (Fernández-Alemán et al., 2013). Οι πρόσφατες εξελίξεις στην τεχνολογία ηλεκτρονικών αρχείων υγείας (EHR) έχουν αυξήσει σημαντικά την ποσότητα κλινικών δεδομένων που μπορούν να ληφθούν ηλεκτρονικά. Αυτά τα δεδομένα περιλαμβάνουν ιατρικά και επιστημονικά έγγραφα, ψηφιακά αρχεία υγείας ασθενών με τα προσωπικά τους δεδομένα και το ιατρικό ιστορικό τους. Επίσης αποτελούν πολύτιμο πόρο για κλινική και μεταφραστική έρευνα (Martinez et al. 2013). Το τυπικό EHR περιλαμβάνει δομημένα δεδομένα, όπως δημοσιογραφικές πληροφορίες ασθενών, διαγνωστικούς κωδικούς ICD-10, εργαστηριακά δεδομένα και ζωτικά σημεία (Austin and Kusumoto, 2016). Δυστυχώς, τα δομημένα δεδομένα αντιπροσωπεύουν μόνο το ένα πέμπτο των διαθέσιμων πληροφοριών περί υγειονομικής περίθαλψης. Δεδομένου ότι οι ιατρικές πληροφορίες είναι συνήθως προσωπικές πληροφορίες, το απόρρητο πρέπει να διασφαλίζεται για δευτερεύουσα χρήση. Ο νόμος περί προστασίας δεδομένων του 1998 και ο νόμος για τα ανθρώπινα δικαιώματα του 1998 επεσήμαναν σαφώς αυτό το σημείο και θεώρησαν τα κλινικά δεδομένα «ευαίσθητα».

Σήμερα, οι γιατροί και ερευνητές συλλέγουν και αποστέλλουν τα EHR σε δημόσιους και ιδιωτικούς οργανισμούς για συντήρηση. Αυτά τα ιδρύματα πρέπει να διασφαλίζουν την υγεία. Οι πληροφορίες που σχετίζονται με τον ασθενή μπορούν να αποκαλυφθούν μόνο με τη συγκατάθεση του ασθενούς. Για ιατρικούς σκοπούς και για σκοπούς στατιστικής ή ιστορικής έρευνας, η Ενότητα 39 του νόμου περί προστασίας δεδομένων επιτρέπει εξαιρέσεις.

Λόγω των αναμενόμενων οφελών, πολλές κυβερνήσεις βασίζονται σε ολοκληρωμένα ηλεκτρονικά αρχεία υγείας. Το 2009, ο πρόεδρος των ΗΠΑ, υπέγραψε το The American Recovery and Reinvestment Act. Αυτό περιλαμβάνει την επένδυση 19 χιλιάδων εκατομμυρίων δολαρίων στις Ηνωμένες Πολιτείες για την ψηφιοποίηση ιατρικών αρχείων. Ακόμη, όπως ανακοίνωσε ο Αντιπρόεδρος της Ευρωπαϊκής Επιτροπής στη συνάντηση υψηλού επιπέδου e-Health του 2010, τα κράτη μέλη της ΕΕ σκοπεύουν επίσης να καταστήσουν τα συστήματα υγείας τους συμβατά έως το 2015. Η Ευρωπαϊκή Ένωση στοχεύει να μοιραστεί τα δεδομένα EHR των ασθενών προκειμένου να ΄ρέει ελευθέρα΄ και να παρέχει ποιοτική και αποτελεσματική ιατρική περίθαλψη (Fernández-Alemán et al., 2013).

2.1.1 Παραδείγματα ηλεκτρονικών αρχείων υγείας

Πρόσφατα, το κέντρο Medicare και Medicaid Services εφάρμοσε πολιτικές για να ενθαρρύνει τη μετάβαση και την αποτελεσματική χρήση των δεδομένων EHR για να αυξήσει το συνολικό ποσοστό δομημένων δεδομένων στα αρχεία υγείας. Ωστόσο, καθώς οι προσβάσιμες ιατρικές πληροφορίες συνεχίζουν να αυξάνονται με διάφορες μορφές, οι προσπάθειες του κέντρου εξυπηρέτησης Medicare και Medicaid είναι απίθανο να έχουν σημαντικό αντίκτυπο στις μορφές δεδομένων και την οργάνωση. Το 1997, το Αμερικάνικο Κολέγιο Καρδιολογίας ίδρυσε το Εθνικό Μητρώο Καρδιαγγειακών Δεδομένων (NCDR) σε μια προσπάθεια τυποποίησης της συλλογής δεδομένων και της αναφοράς για διαγνωστικό καθετηριασμό ή/ και PCI. Έκτοτε, το NCDR έχει εξελιχθεί σε οκτώ τρέχοντα και δύο μελλοντικά μητρώα, τα οποία περιέχουν περισσότερα από 15 εκατομμύρια μοναδικά αρχεία ασθενών, που καλύπτουν το πεδίο της καρδιαγγειακής φροντίδας, όπως χειρουργική επέμβαση παράκαμψης στεφανιαίας αρτηρίας, πυρηνική πνευμονική φλέβα και διάφορα άλλα.

Πρόσφατα, η ACC επέκτεινε το πεδίο των μητρώων της στο περιβάλλον εξωτερικών ασθενών με τη δημιουργία δύο μοναδικών μητρώων: PINNACLE και το Diabetes Collaborative Registry. Το PINNACLE είναι το μεγαλύτερο μητρώο για τη βελτίωση της ποιότητας των κλινικών εξωτερικών ασθενών στην καρδιολογία. Παρακολουθεί τα δεδομένα περισσότερων από 2.500 γιατρών με στεφανιαία νόσο, υπέρταση, καρδιακή ανεπάρκεια και κολπική μαρμαρυγή, καθώς και 15 εκατομμύρια αρχεία ασθενών. Τα δεδομένα από το μητρώο PINNACLE χαρακτηρίζονται ως χρήσιμη χρήση και αναφέρονται αυτόματα στο Σύστημα Αναφοράς Ποιότητας Γιατρού.

Ο νόμος του 2009 για την «Οικονομική και Κλινική Πληροφορική για την Υγεία» (HITECH) αποτελεί μέρος του «Αμερικανικού Νόμου για την Ανάκαμψη και την Επανεπένδυση» και διέθεσε σχεδόν 30 δισεκατομμύρια δολάρια για να ενθαρρύνει τους Αμερικανούς να υιοθετήσουν ηλεκτρονικά αρχεία υγείας (EHR), κυρίως μέσω του προγράμματος "Major Use" (MU) (Gordon and Catalini, 2018). Ως αποτέλεσμα αυτής της προσπάθειας, οι πάροχοι και η χρήση EHR από νοσοκομεία έχουν αυξηθεί δραματικά - ενώ μόνο το 9% των μη ομοσπονδιακών νοσοκομείων οξείας περίθαλψης είχαν βασική EHR το 2008, το 96% είχε EHR έως το 2015 (με το βασικό EHR να ορίζεται ως σύνολο 10 μέτρων που περιλαμβάνουν σημειώσεις γιατρού, λίστες φαρμάκων και λίστες προβλημάτων, μεταξύ άλλων). Δυστυχώς, ενώ η ψηφιοποίηση των ιατρικών αρχείων έχει σαφώς αυξηθεί, η κοινή χρήση ηλεκτρονικών δεδομένων για την υγεία μεταξύ διαφορετικών νοσοκομείων και παροχέων έχει καθυστερήσει πίσω από την υιοθέτηση του EHR, για πολλούς λόγους, συμπεριλαμβανομένων τεχνικών, λειτουργικών και ιδιωτικών προβλημάτων.

2.1.2 Πλεονεκτήματα ηλεκτρονικών αρχείων υγείας

Η ανάλυση της εμπειρίας υγειονομικής περίθαλψης που καταγράφεται στην κλινική βάση δεδομένων, μπορεί να βελτιώσει τη αξιολόγηση των ασθενών, να βελτιώσει τη θεραπεία, να αποφύγει τις ανεπιθύμητες ενέργειες των φαρμάκων και να διασφαλίσει ότι όσοι κινδυνεύουν λαμβάνουν τις κατάλληλες υπηρεσίες υποστήριξης (Martinez et al. 2013). Πρόσφατες προτάσεις υποδηλώνουν ότι τα περιεκτικά αρχεία υγείας μπορούν να αποφέρουν πολλά οφέλη, όπως: μείωση του κόστους, βελτίωση της ποιότητας της

περίθαλψης, ανάπτυξη φαρμάκων βάσει αποδείξεων και διατήρηση αρχείων και αύξηση της κινητικότητας (Fernández-Alemán et al., 2013). Προκειμένου να αποκομίσει αυτά τα οφέλη, το σύστημα EHR πρέπει να πληροί ορισμένες απαιτήσεις όσον αφορά την ακεραιότητα των δεδομένων, την αντίσταση σε αστοχία, την υψηλή διαθεσιμότητα και τη συνέπεια της πολιτικής ασφάλειας.

2.1.3 Μειονεκτήματα ηλεκτρονικών αρχείων υγείας

Τα ιατρικά δεδομένα είναι ποιο εκτεθειμένα και ευάλωτα στην παραβίαση από τυχόν κακόβουλες ενέργειες. Αυτό προκύπτει γιατί είναι πιο εύκολος ο εντοπισμός των συνδυασμών συνθηματικών και κωδικών πρόσβασης, λόγω της μεταβλητότητάς και της υψηλής διαδραστικότητας. Αυτοί οι συνδυασμοί τιμών μπορούν να αξιολογηθούν μαζί και να επιτρέψουν την αποκάλυψη. Η αποκάλυψη ηλεκτρονικών αρχείων υγείας των ασθενών αποτελεί σοβαρή απειλή αφού εμπίπτουν στα ευαίσθητα προσωπικά δεδομένα. Επιπλέον, η επίγνωση των κινδύνων της αποκάλυψης δεδομένων μπορεί να οδηγήσει σε μελλοντική έλλειψη εμπιστοσύνης στη διαθεσιμότητα των ερευνητικών δεδομένων. Το γεγονός ότι τα ιατρικά δεδομένα μπορεί να είναι αδημοσίευτα ή υπερβολικά προστατευμένα για να μειωθεί ο κίνδυνος αποκάλυψης μπορεί να έχει σοβαρές επιπτώσεις στη χρησιμότητά του, καθιστώντας αδύνατη την εξαγωγή οφελών από την ανάλυση. Πιθανά ζητήματα απορρήτου και ασφάλειας: Όπως συμβαίνει με σχεδόν κάθε δίκτυο υπολογιστών σήμερα, τα συστήματα EHR είναι ευάλωτα σε πειρατεία, πράγμα που σημαίνει ότι τα ευαίσθητα δεδομένα των ασθενών ενδέχεται να πέσουν σε λάθος χέρια. Άλλα μειονεκτήματα των ηλεκτρονικών αρχείων υγείας μπορεί να είναι οι ανακριβείς πληροφορίες. Λόγω της στιγμιαίας φύσης των ηλεκτρονικών αρχείων υγείας, πρέπει να ενημερώνονται αμέσως μετά από κάθε επίσκεψη του ασθενούς ή όποτε υπάρχει αλλαγή στις πληροφορίες. Η αποτυχία άμεσης ενημέρωσης μπορεί να οδηγήσει άλλους παροχείς υγειονομικής περίθαλψης να βασιστούν σε ανακριβή δεδομένα κατά τον καθορισμό των κατάλληλων πρωτοκόλλων θεραπείας. Επίσης με τα EHR υπάρχει η πιθανότητα να εκφοβίζονται άσκοπα οι ασθενείς: Επειδή ένα ηλεκτρονικό σύστημα αρχείων υγείας επιτρέπει στους ασθενείς να έχουν πρόσβαση στα ιατρικά τους δεδομένα, μπορεί να δημιουργήσει μια κατάσταση όπου παρερμηνεύουν μια καταχώριση αρχείου. Αυτό μπορεί να προκαλέσει υπερβολικό συναγερμό ή ακόμη και πανικό. Επίσης υπάρχουν αρκετά πιθανά ζητήματα ευθύνης που σχετίζονται με την εφαρμογή του EHR. Για παράδειγμα, τα ιατρικά δεδομένα θα μπορούσαν να χαθούν ή να καταστραφούν κατά τη μετάβαση από ένα χαρτί σε ηλεκτρονικό σύστημα EHR, το οποίο θα μπορούσε να οδηγήσει σε σφάλματα θεραπείας.

2.1.4 Ασφάλεια προσωπικών δεδομένων

Η ανάπτυξη της τεχνολογίας των πληροφοριών και των επικοινωνιών έχει προκαλέσει τα δεδομένα υγείας των ασθενών να αντιμετωπίσουν νέες απειλές για την ασφάλεια και την ιδιωτική ζωή. Οι τρεις βασικοί στόχοι ασφάλειας είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα (CIA) (Haas et al., 2011). Η προστασία και η ασφάλεια των προσωπικών πληροφοριών είναι υψίστης σημασίας για το τμήμα υγείας, επομένως το εκάστοτε σύστημα πρέπει να προστατεύει τις προσωπικές πληροφορίες για την υγεία.

Σύμφωνα με το πρότυπο ISO EN13606, η εμπιστευτικότητα αναφέρεται στη διαδικασία «που διασφαλίζει ότι οι πληροφορίες είναι προσβάσιμες μόνο σε εκείνους που έχουν εξουσιοδότηση να έχουν πρόσβαση σε αυτό». Η ακεραιότητα αναφέρεται στην ευθύνη να διασφαλιστεί ότι οι πληροφορίες είναι ακριβείς και δεν μπορούν να αλλάξουν χωρίς άδεια. Επομένως, η ακεραιότητα των πληροφοριών πρέπει να προστατεύεται για να διασφαλίζεται η ασφάλεια των ασθενών, και ένα σημαντικό στοιχείο αυτής της προστασίας είναι να διασφαλιστεί ο πλήρης έλεγχος ολόκληρου του κύκλου ζωής των πληροφοριών. Η διαθεσιμότητα αναφέρεται στην «ιδιότητα του να είναι προσβάσιμο και να μπορεί να χρησιμοποιηθεί κατόπιν αιτήματος από εξουσιοδοτημένο φορέα». Η διαθεσιμότητα πληροφοριών για την υγεία είναι επίσης κρίσιμη για την αποτελεσματική παροχή ιατρικής περίθαλψης.

Η ασφάλεια περιλαμβάνει επίσης λογοδοσία, πράγμα που σημαίνει ότι οι άνθρωποι έχουν το δικαίωμα να επικρίνουν ή να ρωτούν γιατί συνέβησαν κάποια πράγματα. Πολλοί άνθρωποι πιστεύουν επίσης ότι οι πληροφορίες για την υγεία είναι οι πιο εμπιστευτικές όλων των τύπων προσωπικών πληροφοριών. Επομένως, η προστασία αυτού του απόρρητου είναι πολύ σημαντική για το απόρρητο των ατόμων που μας ενδιαφέρει. Το απόρρητο περιλαμβάνει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα και έχει χαρακτηριστεί ως «η αξίωση ατόμων, ομάδων ή ιδρυμάτων να καθορίσουν από μόνες τους πότε, πώς και σε ποιο βαθμό οι πληροφορίες σχετικά με αυτά κοινοποιούνται σε άλλους» (Westin, 1967).

Η ασφάλεια και το απόρρητο στα EHR ενδέχεται να απειληθούν σοβαρά από χάκερ, ιούς και φυσικές καταστροφές. Τα τελευταία χρόνια, υπήρξαν πολλές φορές απώλειες ή κλοπές ευαίσθητων κλινικών δεδομένων. Για την αντιμετώπιση αυτών των κινδύνων πρέπει να ληφθούν μέτρα για την ενίσχυση της προστασίας δεδομένων EHR, αφού η κατανόηση των δυνατοτήτων ασφάλειας και απορρήτου του συστήματος EHR μπορεί να είναι ζωτικής σημασίας. Οι πολίτες θα πρέπει να γνωρίζουν επίσης τους πιθανούς κινδύνους της κοινοποίησης ηλεκτρονικών ιατρικών αρχείων. Στην Αυστρία, τα άτομα μπορούν ακόμη και να αποφασίζουν εάν τα δεδομένα που σχετίζονται με την υγεία πρέπει να κοινοποιούνται σε υπηρεσίες υγείας και επαγγελματίες υγείας.

Προκειμένου να μετριαστούν αυτές οι ανησυχίες, οργανισμοί όπως η Επιτροπή Πιστοποίησης για την Τεχνολογία Πληροφοριών Υγείας (CCHIT) προσφέρουν ένα πρόγραμμα το οποίο περιλαμβάνει αυστηρές επιθεωρήσεις πτυχών ασφάλειας βάσει των υφιστάμενων προτύπων που σχετίζονται κυρίως με τις Ηνωμένες Πολιτείες. Η CCHIT πιστοποιεί την τεχνολογία EHR από το 2006. Η παροχή πρόσβασης σε ηλεκτρονικά ιατρικά αρχεία είναι το πρώτο βήμα για την ενεργοποίηση της φροντίδας των ασθενών και τη βελτίωση του συστήματος υγείας. Ωστόσο, αυτό δημιουργεί νέες απειλές για την ασφάλεια. Αυτό που είναι πραγματικά ανησυχητικό είναι ότι τόσο τα άτομα όσο και οι οντότητες μπορούν να έχουν πρόσβαση σε ηλεκτρονικά ιατρικά αρχεία ασθενών. Οι ευπάθειες ασφάλειας σε ορισμένα από αυτά τα συστήματα ενδέχεται να προκαλέσουν την αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα ή εταιρείες. Επομένως, τα δεδομένα υγείας πρέπει να προστατεύονται από παραβίαση, μη εξουσιοδοτημένη πρόσβαση και κατάχρηση, η οποία περιλαμβάνει θέματα απορρήτου, αξιοπιστίας, ελέγχου ταυτότητας, ευθύνης και διαθεσιμότητας. Τα ηλεκτρονικά ιατρικά αρχεία είναι επίσης δύσκολο να διατηρηθεί η εμπιστευτικότητα των δεδομένων τους, για παράδειγμα

το διοικητικό προσωπικό μπορεί να έχει πρόσβαση σε πληροφορίες χωρίς τη ρητή συγκατάθεση του ασθενούς.

2.2 Big Data

Ο όρος Big Data προτάθηκε για πρώτη φορά από τους επιστήμονες της ΝΑΣΑ το 1997 για να περιγράψει τη δυσκολία το μέγεθος δεδομένων που είναι πολύ μεγάλος για να αποθηκευτούν στην κύρια μνήμη του υπολογιστή, περιορίζοντας έτσι την ανάλυση ολόκληρου του συνόλου δεδομένων (Austin and Kusumoto, 2016). Αν και υπάρχουν πολλοί ορισμοί, οι περισσότεροι από τους ορισμούς το αντιπροσωπεύουν ως σύνολο δεδομένων που είναι πολύ μεγάλο για εύκολη επεξεργασία και διαχείριση. Τα Big Data περιγράφουν επίσης τις δραστηριότητες συλλογής, αποθήκευσης, ανάλυσης και μετεγκατάστασης μεγάλων ποσοτήτων δεδομένων. Αν και η φράση είναι σχετικά νέα, δεν είναι μια έννοια συλλογής και ανάλυσης δεδομένων μεγάλης κλίμακας. Βασικά, η έννοια των Big Data σχετίζεται με τους διαθέσιμους πόρους σε μια δεδομένη στιγμή.
Αναλύοντας τα μεγάλα δεδομένα των σημερινών μεγάλων όγκων δεδομένων, οι κάτοχοι δεδομένων μπορούν να αναζητήσουν δημόσια νήματα που συνδέουν φαινομενικά άσχετα σημεία δεδομένων για να εντοπίσουν συσχετίσεις που διαφορετικά δεν θα είχαν παρατηρηθεί. Τα Big Data δεν μπορούν να εξηγήσουν γιατί ή πως λειτουργούν αυτές οι συσχετίσεις, αλλά προειδοποιεί τους ερευνητές να πραγματοποιήσουν περαιτέρω ανάλυση ή προοπτικές μελέτες για να απαντήσουν σε ερωτήσεις που δεν έχουν απαντηθεί πριν. Ο στόχος της μεγάλης επισκεψιμότητας δεδομένων είναι η απελευθέρωση της αξίας των μεγάλων όγκων δεδομένων σε μια προσπάθεια βελτίωσης της λήψης αποφάσεων, της αποτελεσματικότητας, των αποτελεσμάτων και του χρόνου παράδοσης των κατόχων των δεδομένων.

2.2.1 Big Data analytics

Αν ένας γιατρός, πριν από πολλά χρόνια, είδε ασθενή που έπασχε από μια σπάνια ασθένεια και αναρωτήθηκε εάν υπήρχαν παρόμοιοι ασθενείς που έπασχαν από την ίδια ασθένεια, το Big Data analytics θα μπορούσε να τον βοηθήσει να αποκτήσει γνώση της εξέλιξης της νόσου ή των θεραπευτικών αποτελεσμάτων. Η Big Data analytics μπορεί να παρέχει άμεσες απαντήσεις σε αυτά τα ερωτήματα, αυξάνοντας έτσι τη βάση γνώσεων και ενδεχομένως ενθαρρύνοντας τη συνεργασία και την εκμάθηση μαθημάτων (Austin and Kusumoto, 2016). Οι εξαιρετικά καθορισμένες ερωτήσεις μπορούν να εντοπίσουν μη αναγνωρισμένους ασθενείς που πληρούν τα κριτήρια συμπερίληψης τυχαιοποιημένων ελεγχόμενων δοκιμών κατά την αξιολόγηση της σκοπιμότητας του σχεδιασμού της μελέτης. Αυτά τα ερωτήματα θα ξεκινήσουν επίσης την πρόσληψη μόλις ληφθεί η έγκριση του διοικητικού συμβουλίου θεσμικής αναθεώρησης.
Το Big Data analytics δεν χρησιμοποιείται μόνο για την παρακολούθηση ατόμων, αλλά και για έρευνα πληθυσμού. Η φιλόδοξη μελέτη Health eHeart του Πανεπιστημίου της Καλιφόρνιας-Σαν Φρανσίσκο στοχεύει στον προσδιορισμό του προγνωστικού μοτίβου των καρδιακών παθήσεων, στον προσδιορισμό της αιτίας της κολπικής μαρμαρυγής, στη μείωση του αριθμού των ασθενών με καρδιακή ανεπάρκεια και στον προσδιορισμό της

επίδρασης των κοινωνικών μέσων στην υγεία της καρδιάς αναλύοντας έως 1 εκατομμύριο συμμετέχοντες άνω των 10 ετών.

2.2.2 Απειλές για την προστασία δεδομένων

Καθώς η ιατρική κοινότητα αναγνωρίζει την αξία της μεγάλης ποσότητας δεδομένων των ασθενών και στην προώθηση τους, άλλοι έχουν βρει τα Big Data ως τρόπο παραβίασης αυτών των δεδομένων. Παρά την προστασία που παρέχεται από τον Νόμο για τη φορητότητα και την υπευθυνότητα της ασφάλισης υγείας του 1996, οι παραβιάσεις ασφάλειας έχουν γίνει κοινές τα τελευταία χρόνια. Εκείνοι που επηρεάστηκαν από τέτοιες παραβιάσεις περιλαμβάνουν και τον ασφαλιστικό γίγαντα Anthem (80 εκατομμύρια εγγραφές σε κίνδυνο), το UCLA Health System (4,5 εκατομμύρια εγγραφές σε κίνδυνο) και το Healthcare.gov (δοκιμαστικός διακομιστής, χωρίς αρχεία σε κίνδυνο). Τα δεδομένα διακομιστή συνήθως δεν είναι αναγνωρίσιμα ή κρυπτογραφημένα και περιλαμβάνει δημογραφικές πληροφορίες και αριθμούς κοινωνικής ασφάλισης που στοχεύουν σε εγκληματίες στον κυβερνοχώρο. Παρά τις προσπάθειες για τον εντοπισμό ευαίσθητων ιατρικών πληροφοριών για ευρεία διάδοση, υπάρχει η απειλή του επαναπροσδιορισμού δεδομένων και έχει αποδειχθεί ότι η πιθανότητα επιτυχούς επαναπροσδιορισμού ενός μεμονωμένου αρχείου μπορεί να είναι μικρότερη από 0,01%. Η από κοινού λήψη αποφάσεων μεταξύ ασθενών και παροχέων είναι ζωτικής σημασίας για την επιτυχή εφαρμογή νέων προγνωστικών εργαλείων και στρατηγικών θεραπείας με βάση την ανάλυση.
Οι οργανισμοί υγειονομικής περίθαλψης αποθηκεύουν, συντηρούν και μεταδίδουν μεγάλες ποσότητες δεδομένων για να υποστηρίξουν την παροχή αποτελεσματικής και κατάλληλης φροντίδας. Ωστόσο, η προστασία αυτών των δεδομένων αποτελεί τρομακτική απαίτηση εδώ και δεκαετίες. Η βιομηχανία υγειονομικής περίθαλψης παραμένει μια από τις πιο ευάλωτες παραβιάσεις δεδομένων στο κοινό. Στην πραγματικότητα, οι 'εισβολείς' μπορούν να χρησιμοποιήσουν μεθόδους και διαδικασίες εξόρυξης δεδομένων για να βρουν ευαίσθητα δεδομένα και να τα διανείμουν στο κοινό, προκαλώντας έτσι διαρροή δεδομένων. Παρόλο που η εφαρμογή μέτρων ασφαλείας εξακολουθεί να είναι μια περίπλοκη διαδικασία, καθώς η υπέρβαση των μεθόδων ελέγχου ασφάλειας γίνεται όλο και πιο περίπλοκη, είναι πάντα σε κίνδυνο. Ως εκ τούτου, είναι σημαντικό να οργανωθεί η εφαρμογή λύσεων ασφάλειας ιατρικών δεδομένων για την προστασία σημαντικών περιουσιακών στοιχείων, ενώ πληρούνται οι απαιτήσεις ιατρικής συμμόρφωσης.

2.3 Άλλες μορφές αρχείων υγείας

Η συλλογή δεδομένων EHR είναι μόνο η κορυφή του παγόβουνου. Οι φορητές συσκευές όπως το Fitbit Surge (Fitbit, CA, CA) και το Apple iWatch (Apple, Cupertino CA) γίνονται όλο και πιο δημοφιλή και είναι σε θέση να συλλέγουν και να αποθηκεύουν δεδομένα J Interv Card Electrophysiol (2016), σε παροχείς υγειονομικής περίθαλψης και το ιατρικό δίκτυο. Συνήθως είναι δυνατή η συλλογή άλλων σχετικών δεδομένων μέσω της χρήσης

του Διαδικτύου, των μέσων κοινωνικής δικτύωσης και της θέσης GPS, ή λιγότερο συχνά μέσω της χρήσης αλληλουχίας τηλεϊατρικής και γονιδίων.
Μετά την Ευρώπη, τον Καναδά, την Αυστραλία, τη Ρωσία και τη Λατινική Αμερική, η Sophia Genetics, παγκόσμιος ηγέτης στην Ιατρική βάσει δεδομένων , ανακοίνωσε στην πιο πρόσφατη ετήσια συνάντηση με το Αμερικάνικο Κολέγιο Ιατρικής Γενετικής και Γονιδιωματικής του 2017 (ACMG) ότι η τεχνητή νοημοσύνη του έχει υιοθετηθεί από αφρικανικά νοσοκομεία για την προώθηση της φροντίδας των ασθενών σε ολόκληρη την αφρικανική ήπειρο. Στο Μαρόκο, για παράδειγμα, η PharmaProcess στην Καζαμπλάνκα, το ImmCell, το Ογκολογικό Κέντρο Al Azhar και το Κέντρο Βιολογίας Riad στη Ραμπάτ είναι ορισμένα ιατρικά ιδρύματα στην πρώτη γραμμή της καινοτομίας που έχουν αρχίσει να ενσωματώνουν τη Sophia για την επιτάχυνση και την ανάλυση των γονιδιωματικών δεδομένων για την ανίχνευση μεταλλάξεων που προκαλούν ασθένειες στο προφίλ γονιδιώματος του ασθενούς και καθορίζουν την πιο αποτελεσματική θεραπεία (Abouelmehdi et al., 2017). Καθημερινά η τεχνολογική ανάπτυξη είναι ραγδαία, έτσι και οι ιατρικές πληροφορίες που συλλέγονται αυξάνονται καθημερινά. Υπολογίζοντας αυτους τους ρυθμούς ανάπτυξης οι ιατρικές πληροφορίες πιθανότατα θα αυξηθούν, ως προς το είδος αλλά και το μέγεθος των αρχείων υγείας. Η προστασία τους και η διασφάλιση τους είναι κάτι που ήδη προβληματίζει και πρέπει ληφθεί σοβαρά υπόψη.

2.4 Προστασία Ασφάλειας Δεδομένων Υγείας

Χρησιμοποιούνται διάφορες τεχνολογίες για την προστασία της ασφάλειας και της ιδιωτικής ζωής των ιατρικών δεδομένων. Οι πιο ευρέως χρησιμοποιούμενες τεχνολογίες είναι (Abouelmehdi et al., 2017):

2.4.1 Επαλήθευση ταυτότητας

Η επαλήθευση ταυτότητας είναι να αποδείξει ή να επιβεβαιώσει ότι οι ισχυρισμοί που διατυπώνονται από τον χρήστη για το θέμα ή κατά του θέματος είναι αληθείς και αυθεντικοί. Παίζει ζωτικό ρόλο σε οποιονδήποτε οργανισμό: προστασία της πρόσβασης στο δίκτυο της εταιρείας, προστασία της ταυτότητας των χρηστών και διασφάλιση ότι οι χρήστες είναι αυτοί που ισχυρίζονται ότι είναι. Τα περισσότερα κρυπτογραφικά πρωτόκολλα περιλαμβάνουν κάποια μορφή ελέγχου ταυτότητας τελικού σημείου ειδικά σχεδιασμένη 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 πρωτόκολλα κρυπτογράφησης που μπορούν να παρέχουν ασφάλεια για επικοινωνίες σε δίκτυα όπως το Διαδίκτυο.
Τα TLS και SSL κρυπτογραφούν τη σύνδεση δικτύου στο επίπεδο μεταφοράς από άκρο σε άκρο. Πολλές εκδόσεις του πρωτοκόλλου χρησιμοποιούνται ευρέως σε εφαρμογές όπως η περιήγηση στο Web, το ηλεκτρονικό ταχυδρομείο, το φαξ στο Διαδίκτυο, τα άμεσα μηνύματα και το Voice over IP (VoIP). Μπορείτε να χρησιμοποιήσετε SSL ή TLS για τον έλεγχο ταυτότητας του διακομιστή με μια αμοιβαία αξιόπιστη αρχή ελέγχου ταυτότητας. Επιπλέον, ο αλγόριθμος Bull Eye μπορεί να χρησιμοποιηθεί για την παρακολούθηση όλων των ευαίσθητων πληροφοριών. Αυτός ο αλγόριθμος έχει χρησιμοποιηθεί για τη

διασφάλιση της ασφάλειας των δεδομένων και τη διαχείριση της σχέσης μεταξύ των αρχικών δεδομένων και των αναπαραγόμενων δεδομένων. Μόνο εξουσιοδοτημένο προσωπικό επιτρέπεται να διαβάζει ή να προσθέτει κρίσιμα δεδομένα. Παρέχεται διαγραφή επικοινωνίας του κωδικού πρόσβασης μεταξύ διακομιστών. Στο σύστημα υγειονομικής περίθαλψης, είναι απαραίτητο να επαληθεύονται οι πληροφορίες υγειονομικής περίθαλψης που παρέχονται από τον παροχέα και την ταυτότητα του καταναλωτή κάθε φορά που πραγματοποιείται μια επίσκεψη.

2.4.2 Κρυπτογράφηση

Η κρυπτογράφηση δεδομένων είναι ένα αποτελεσματικό μέσο για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα δεδομένα. Η λύση του προστατεύει και διατηρεί την ιδιοκτησία δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής του - από το κέντρο δεδομένων έως τα τελικά σημεία (συμπεριλαμβανομένων των κινητών συσκευών που χρησιμοποιούνται από γιατρούς, κλινικούς και διαχειριστές) και στο cloud. Η κρυπτογράφηση είναι χρήσιμη για την αποφυγή ζημιών (όπως κλοπή συσκευών αποθήκευσης).
Οι οργανισμοί ή οι παροχείς υγειονομικής περίθαλψης πρέπει να διασφαλίσουν ότι τα συστήματα κρυπτογράφησης είναι αποτελεσματικά, εύχρηστα από ασθενείς και επαγγελματίες υγείας και επεκτείνονται εύκολα ώστε να συμπεριλαμβάνουν νέα ηλεκτρονικά ιατρικά αρχεία. Επιπλέον, πρέπει να ελαχιστοποιηθεί ο αριθμός των πλήκτρων που κρατά κάθε κόμμα. Αν και έχουν αναπτυχθεί διάφοροι αλγόριθμοι κρυπτογράφησης σχετικά καλά (RSA, Rijndael, AES και RC6 20, 22, 23, DES, 3DES, RC4 21, IDEA, Blowfish…), η σωστή επιλογή των κατάλληλων αλγορίθμων κρυπτογράφησης για την επιβολή ασφαλούς αποθήκευσης παραμένει ένα δύσκολο πρόβλημα, το οποίο είναι ανάλογο με το είδος των πληροφοριών που θα αποθηκεύονται.

2.4.3 Κάλυψη δεδομένων

Η απόκρυψη αντικαθιστά ευαίσθητα δεδομένα με μη αναγνωρισμένες τιμές, αλλά αυτή δεν είναι πραγματική τεχνολογία κρυπτογράφησης, επομένως η κρυφή τιμή δεν μπορεί να επιστραφεί στην αρχική τιμή. Χρησιμοποιείτε μια στρατηγική για τον εντοπισμό συνόλων δεδομένων και την απόκρυψη προσωπικών αναγνωριστικών (όπως ονόματα, αριθμούς κοινωνικής ασφάλισης) και απαγόρευση των αναγνωριστικών (όπως δεδομένα γέννησης και ταχυδρομικοί κώδικες). Επομένως, η αποκάλυψη δεδομένων είναι μια από τις πιο δημοφιλείς μεθόδους για την ανωνυμοποίηση δεδομένων σε πραγματικό χρόνο. Η k-ανωνυμία που προτάθηκε αρχικά από τους Swaney και Samrati μπορεί να αποτρέψει τη διαρροή ταυτότητας, αλλά δεν μπορεί να αποτρέψει τη διαρροή χαρακτηριστικών.
Οι Truta et al. έχουν παρουσιάσει ευαισθησία που προστατεύει τόσο από την ταυτότητα όσο και από την αποκάλυψη χαρακτηριστικών. Άλλες μέθοδοι ανωνυμίας περιλαμβάνουν την προσθήκη θορύβου στα δεδομένα, την ανταλλαγή κελιών σε στήλες και την αντικατάσταση της κατηγορίας της ομάδας εγγραφής k με k αντίγραφα ενός μεμονωμένου πράκτορα. Αυτές οι μέθοδοι έχουν ένα κοινό πρόβλημα ότι είναι δύσκολο να ανωνυμοποιηθούν σύνολα δεδομένων υψηλών διαστάσεων. Ένα σημαντικό όφελος αυτής της τεχνολογίας είναι ότι μειώνει το κόστος προστασίας της μεγάλης κλίμακας

ανάπτυξης δεδομένων. Δεδομένου ότι τα ασφαλή δεδομένα μεταδίδονται από μια ασφαλή πηγή στην πλατφόρμα, η απόκρυψη μπορεί να μειώσει την ανάγκη εφαρμογής άλλων ελέγχων ασφαλείας στα δεδομένα της πλατφόρμας.

2.4.4 Έλεγχος Πρόσβασης

Μόλις γίνει έλεγχος ταυτότητας, οι χρήστες μπορούν να έχουν πρόσβαση στο σύστημα πληροφοριών, αλλά η πρόσβασή τους θα εξακολουθεί να υπόκειται σε πολιτικές ελέγχου πρόσβασης, οι οποίες βασίζονται συνήθως στα προνόμια και τα δικαιώματα οποιουδήποτε εξουσιοδοτημένου από τον ασθενή ή αξιόπιστου τρίτου ατόμου. Επομένως, είναι ένας ισχυρός και ευέλικτος μηχανισμός άδειας χρήστη. Παρέχει προηγμένο έλεγχο εξουσιοδότησης για να διασφαλίσει ότι οι χρήστες μπορούν να εκτελούν μόνο δραστηριότητες για τις οποίες έχουν εξουσία, όπως πρόσβαση δεδομένων, υποβολή εργασίας, διαχείριση συμπλεγμάτων κ.λπ.
Έχουν προταθεί πολλές λύσεις για την επίλυση θεμάτων ασφάλειας και ελέγχου πρόσβασης. Ο έλεγχος πρόσβασης βάσει ρόλου (RBAC) και ο έλεγχος πρόσβασης βάσει λειτουργιών (ABAC) είναι τα πιο δημοφιλή μοντέλα EHR. Τα RBAC και ABAC παρουσιάζουν ορισμένους περιορισμούς όταν χρησιμοποιούνται μόνα τους σε ιατρικό σύστημα. Προκειμένου να πληρούνται οι απαιτήσεις του λεπτομερούς ελέγχου πρόσβασης, αλλά και για τη διατήρηση της ασφάλειας και του απορρήτου, συνιστούμε τη χρήση τεχνολογιών σε συνδυασμό με άλλες τεχνολογίες ασφαλείας, όπως μεθόδους κρυπτογράφησης και ελέγχου πρόσβασης.

2.4.5 Blockchain

Η τεχνολογία Blockchain είναι μια νέα τεχνική λύση που υιοθετήθηκε από την πρώτη ομάδα χρηστών (Katuwal et al., 2018). Μία από τις προκλήσεις είναι ακόμα πώς να καταστήσει την κορυφαία λύση της τεχνολογίας blockchain σύμφωνα με τους υπάρχοντες κανονισμούς και πρότυπα. Ενώ τα υπάρχοντα συστήματα HIE έχουν πολλά χρόνια για να εξελιχθούν προς την ικανοποίηση των κανονιστικών απαιτήσεων, η τεχνολογία blockchain μπορεί να βρίσκεται ακόμη στη φάση εξέλιξης για να βρει το καλύτερο σημείο προσγείωσης στην περιοχή υγειονομικής περίθαλψης, όπου μπορείτε επίσης να συμμορφωθείτε πλήρως για να αναπτύξετε πρότυπα και κανονισμούς περίθαλψης. Για το σκοπό αυτό, οι παροχείς λύσεων πρέπει να εξετάσουν πολλές πιλοτικές εφαρμογές και πρέπει να εξετάσουν τον αυστηρό έλεγχο και την επαλήθευση των υποκείμενων τεχνικών στοιχείων. Οι κανονιστικές απαιτήσεις μπορούν επίσης να προωθήσουν περαιτέρω τεχνολογική πρόοδο στην τεχνολογία blockchain.
Οι πρόσφατα ισχύουσες απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) είναι μία από τις περιπτώσεις που πυροδότησαν συζητήσεις και σκέψεις σχετικά με τον τρόπο περαιτέρω ανάπτυξης της τεχνολογίας blockchain για συμμόρφωση με τους καθιερωμένους κανονισμούς. Το Blockchain και το GDPR έχουν διπλή σχέση. Από τη μία πλευρά, για παράδειγμα, το GDPR ορίζει το δικαίωμα διαγραφής / δικαίωμα λήψης, το οποίο δίνει στο άτομο (τον δημιουργό δεδομένων) πλήρη δικαιώματα και το δικαίωμα ελέγχου των δεδομένων του, τα οποία έρχονται σε άμεση σύγκρουση με τη συνεχώς μεταβαλλόμενη φύση του blockchain. Τα δεδομένα της υγειονομικής περίθαλψης

συνήθως αποθηκεύονται εκτός αλυσίδας και μόνο οι δείκτες προς τα δεδομένα (συνήθως τα κρυπτογραφημένα κομμάτια του) αποθηκεύονται στο blockchain. Αυτή η προσέγγιση παρέχει έναν τρόπο για να κάνουν τις εφαρμογές blockchain συμβατές με το GDPR.
Πρέπει να εξεταστεί προσεκτικά η ενσωμάτωση κανονισμών GDPR στις εφαρμογές blockchain. Από την άλλη πλευρά, όσον αφορά την αποκέντρωση, κανονισμοί όπως το GDPR μπορούν με το blockchain να είναι τέλειοι συνεργάτες. Καθώς οι χρήστες συνειδητοποιούν τα προσωπικά τους δεδομένα και εφαρμόζουν κανονισμούς απορρήτου, αυξάνεται το ενδιαφέρον για τα δεδομένα υγειονομικής περίθαλψης που ελέγχονται από τους ασθενείς. Δεδομένου ότι υπάρχουν φιλικές προς το χρήστη εφαρμογές που χρησιμοποιούν την κατάλληλη ασφάλεια και κίνητρα για τη διαχείριση προσωπικών δεδομένων, τα άτομα μπορούν να έχουν πρόσβαση και να ελέγχουν δεδομένα υγειονομικής περίθαλψης και μπορούν να συμμετέχουν στην παγκόσμια ανταλλαγή δεδομένων που απαιτείται για υπηρεσίες blockchain έρευνας και υγειονομικής περίθαλψης.

Η εταιρεία Blockchain VeChain ανακοίνωσε ότι συνεργάστηκε με το I-Dante της Κύπρου για τη δημιουργία μιας πλατφόρμας διαχείρισης ιατρικών δεδομένων blockchain (Ledger Insights, 2020). Η πλατφόρμα ονομάζεται E-NewHealthLife και θα χρησιμοποιηθεί από το Mediteranean Hospital στην Κύπρο για να επιτρέψει στους ασθενείς να μοιράζονται με ασφάλεια δεδομένα υγείας. Το E-NewHealthLife θα παρουσιαστεί στην κλινική έκτακτης ανάγκης του Κυπριακού νοσοκομείου. Οι ασθενείς θα λάβουν μια κρυπτογραφημένη κάρτα NFC, η οποία θα λειτουργεί ως ψηφιακό ιατρικό διαβατήριο, επιτρέποντάς τους να αναγνωριστούν στο γραφείο εγγραφής, να χρησιμοποιήσουν την εφαρμογή για να ελέγξουν πού βρίσκονται στη γραμμή και να διαχειρίζονται τα ιατρικά τους αρχεία με ασφάλεια.
Όπως και οι περισσότερες λύσεις, το blockchain είναι μέρος ενός μεγαλύτερου έργου, επομένως τα ηλεκτρονικά δεδομένα υγείας δεν θα αποθηκεύονται στην αλυσίδα. Σε αυτήν την περίπτωση, η λύση blockchain έχει δύο λειτουργίες. Το ένα είναι να επιτρέπεται η πρόσβαση σε δεδομένα ιατρικών αρχείων. Το άλλο είναι μέρος του ψηφιακού μετασχηματισμού του νοσοκομείου που του επιτρέπει να συλλέγει λεπτομερή δεδομένα. Για παράδειγμα, όταν κάποιος επισκέπτεται την αίθουσα έκτακτης ανάγκης ενός νοσοκομείου, πρέπει να εγγραφεί στον τόπο έκδοσης της κάρτας NFC. Στη συνέχεια υπάρχει η χειρουργική επέμβαση που ανατίθενται στον γιατρό και συνήθως πρέπει να ελέγχουν τα στοιχεία. Σε συνδυασμό με την εφαρμογή, μια λύση συμβατή με το GDPR επιτρέπει στους ασθενείς να έχουν πλήρη έλεγχο του ποιος βλέπει τα αρχεία υγείας τους. Μεταξύ άλλων έργων ρεκόρ υγείας, το Υπουργείο Υγείας και Πρόληψης των ΗΑΕ χρησιμοποιεί το blockchain για την αποθήκευση δεδομένων υγείας και ιατρικής. Το Νοσοκομείο της Ταϊπέι που συνδέεται με το Ιατρικό Πανεπιστήμιο της Ταϊπέι εργάζεται πάνω σε ένα έξυπνο διαβατήριο υγείας για να μοιράζεται ιατρικά δεδομένα. Και η IBM συνεργάζεται με το University Health Network του Καναδά σε μια πλατφόρμα εγγραφών υγείας blockchain.

Κεφάλαιο 3

3.1 Διεθνή και Ευρωπαϊκό Νομοθετικό Πλαίσιο Προστασίας Προσωπικών Δεδομένων (GDPR)

Η τεχνολογία καθημερινά αναβαθμίζεται έχοντας επιρροή σε όλες τις επιστήμες με μεγάλη επιτυχία, σε σημείο όπου η παρουσία της κρίνεται πλέον απαραίτητη. Όπως είναι φυσικό αυξήθηκαν σημαντικά ο όγκος των πληροφοριών, οι ηλεκτρονικές πληροφορίες και τα δεδομένα προσωπικού χαρακτήρα. Έτσι αναπόφευκτα οι τεχνολογικές εξελίξεις και η παγκοσμιοποίηση δημιούργησαν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Οι ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων είχαν ως αποτέλεσμα μεταρρυθμίσεις της ισχύουσας νομοθεσίας στην Ευρωπαϊκή Ένωση (ΕΕ). Έτσι γεννιέται και η ανάγκη για τη δημιουργία ενός νέου κανονισμού προσαρμοσμένο στα σημερινά δεδομένα από την ΕΕ, ο κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR – General Data Protection Regulation). Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) είναι ένας νέος πανευρωπαϊκός νόμος που αντικαθιστά το Νόμο περί Προστασίας Δεδομένων του 1998 στο Ηνωμένο Βασίλειο. Είναι μέρος του ευρύτερου πακέτου προστασίας δεδομένων που περιλαμβάνεται στον Νόμο περί προστασίας δεδομένων. Ο GDPR ισχύει για "προσωπικά δεδομένα", δηλαδή για κάθε πληροφορία που σχετίζεται με αναγνωρίσιμες ταυτότητες που μπορούν να αναγνωριστούν άμεσα ή έμμεσα, ειδικά πληροφορίες που μπορούν να προσδιοριστούν με αναφορά αναγνωριστικών. Ο κανονισμός αυτός στοχεύει στη μεταρρύθμιση των υφιστάμενων μέτρων για το θέμα της προστασίας των προσωπικών δεδομένων, των πολιτών της Ευρωπαϊκής Ένωσης, με μεγάλη συμβολή στα δικαιώματα και τις ελευθερίες των ανθρώπων και στη θέσπιση κανόνων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Μετά μια τετραετή διαπραγμάτευση, στις 22 Οκτωβρίου 1995, θεσπίστηκε η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία ενσωματώθηκε στην εθνική έννομη τάξη μας με τον ν 2472/1997. Έτσι, μέσω μιας διαδικασίας μακροπρόθεσμης ανάπτυξης, η Ευρωπαϊκή Ένωση απέκτησε με επιτυχία δικαιώματα προστασίας για να αποτρέψει την αθέμιτη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ωστόσο, με την πάροδο του χρόνου, ειδικά υπό την πίεση νέων τεχνολογιών, αυτή η προστασία φέρνει νέες προκλήσεις και νέους κινδύνους για τα προσωπικά δεδομένα. Επομένως, θεωρήθηκε λοιπόν απαραίτητος ο εκσυγχρονισμός της Οδηγίας 95/46/ΕΚ και η μεταρρύθμισή της σε ένα Γενικό Κανονισμό. Έτσι, στις 6 Απριλίου 2016, ψηφίστηκε ο Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων ΕΕ 2016/679, ο οποίος αντικατέστησε την Οδηγία, η οποία εκδόθηκε πριν από είκοσι χρόνια.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679 (GDPR) είναι ένας κανονισμός της νομοθεσίας της ΕΕ για την προστασία δεδομένων και την προστασία της ιδιωτικής ζωής στην Ευρωπαϊκή Ένωση (ΕΕ) και τον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ). Αφορά επίσης τη διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός των περιοχών της ΕΕ και του ΕΟΧ. Ο GDPR καλύπτει όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης: Αυστρία, Βέλγιο, Βουλγαρία, Κροατία, Κύπρος, Τσεχική Δημοκρατία, Δανία, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιρλανδία, Ιταλία, Λετονία, Λιθουανία, Λουξεμβούργο, Μάλτα, Κάτω Χώρες, Πολωνία, Πορτογαλία, Ρουμανία, Σλοβακία, Σλοβενία, Ισπανία και Σουηδία.

Δεδομένου ότι το Ηνωμένο Βασίλειο εξακολουθεί να αποτελεί μέρος της Ευρωπαϊκής Ένωσης (επί του παρόντος), τα Channel Isles, England, Βόρεια Ιρλανδία, Σκωτία και Ουαλία, διέπονται επίσης από τον GDPR. Εκτός από τα κράτη μέλη, ο GDPR καλύπτει τις χώρες του Ευρωπαϊκού Οικονομικού Χώρου: Ισλανδία, Λιχτενστάιν και Νορβηγία (Reciprocitylabs, 2019).

Το GDPR στοχεύει κυρίως στον έλεγχο των προσώπων έναντι των προσωπικών τους δεδομένων και στην απλούστευση του ρυθμιστικού περιβάλλοντος για τις διεθνείς επιχειρήσεις, ενοποιώντας τον κανονισμό εντός της ΕΕ. Αντικαθιστώντας την οδηγία 95/46 / ΕΚ για την προστασία των δεδομένων, ο κανονισμός περιέχει διατάξεις και απαιτήσεις σχετικά με την επεξεργασία προσωπικών δεδομένων ατόμων (που ονομάζονται επίσημα υποκείμενα δεδομένων στο GDPR) και διαμένουν στον ΕΟΧ και ισχύει για κάθε επιχείρηση - την τοποθεσία και την ιθαγένεια ή την κατοικία των υποκειμένων των δεδομένων - η οποία επεξεργάζεται τις προσωπικές πληροφορίες των υποκειμένων των δεδομένων στο εσωτερικό του ΕΟΧ.

Το GDPR εγκρίθηκε στις 14 Απριλίου 2016 μετά από τέσσερα χρόνια σύνταξης, πίεσης και διαπραγματεύσεων μεταξύ των κρατών μελών της ΕΕ και πολλών επηρεαζόμενων οργανισμών. Συμφώνησε και οριστικοποιήθηκε στις 14 Απριλίου του 2016, ενώ στις 4 Μαΐου 2016 δημοσιεύθηκε το τελικό του κείμενο στην επίσημη εφημερίδα της Ευρωπαϊκής Ένωσης. Δόθηκε μια περίοδος προσαρμογής, μελέτης και εφαρμογής του κανονισμού και κατέστη εκτελεστό από τις 25 Μαΐου 2018 και έκτοτε, έχει άμεσο αντίκτυπο στα κράτη μέλη και άνοιξε ένα νέο κεφάλαιο στο ενωσιακό δίκαιο για την προστασία των προσωπικών δεδομένων.

Εφόσον το GDPR είναι κανονισμός και όχι οδηγία, είναι άμεσα δεσμευτικός και εφαρμόσιμος, αλλά παρέχει ευελιξία για ορισμένες πτυχές του κανονισμού που πρέπει να προσαρμόζονται μεμονωμένα, έτσι η κάθε χώρα μέλος της Ε.Ε. μπορεί να προσαρμόσει το κανονισμό ανάλογα με τη νομοθεσία της και φυσικά την έγκριση από την Ε.Ε. Ο κανονισμός έγινε ένα πρότυπο πολλών εθνικών νόμων εκτός της ΕΕ, όπως η Χιλή, η Ιαπωνία, η Βραζιλία, η Νότια Κορέα, η Αργεντινή και η Κένυα. Η εισαγωγή του GDPR αποσκοπούσε στην αντικατάσταση, της οδηγίας για προστασία δεδομένων 95/46 / ΕΚ (DPD) που εισήχθη το 1995 και, ως οδηγία, άφηνε κάποιο περιθώριο παρερμηνείας και ασάφειας για τη μεταφορά πληροφοριών προσωπικών δεδομένων και με τα σημερινά δεδομένα κρίθηκε ακατάλληλη και ανεπαρκής. Επιπλέον, η ταχεία αλλαγή της οδηγίας οφείλεται στο τοπίο δεδομένων που προκλήθηκε από την έκρηξη παντού από φορητούς υπολογιστές και τη μεγάλη αύξηση των δεδομένων. Ωστόσο, οι ριζοσπαστικές αλλαγές που επέφερε το GDPR επηρεάζει σοβαρά τις επιχειρήσεις που λειτουργούν εντός και

εκτός της επικράτειας της ΕΕ. Ο Νόμος αυτός όπως είναι φυσικό, έχει τεθεί σε εφαρμογή και στο τομέα της υγειονομικής περίθαλψης. Η ταχεία ανάπτυξη της ψηφιακής υγείας αποτελεί κρίσιμη πρόκληση για την προστασία των προσωπικών δεδομένων των ασθενών, αφού πλέον οι πληροφορίες που παράγονται για την υγεία είναι αρκετές και σημαντικές.
Ο γενικός κανονισμός για την προστασία των δεδομένων (GDPR) στοχεύει στη μεταρρύθμιση των υφιστάμενων μέτρων για την προστασία των προσωπικών δεδομένων των πολιτών της Ευρωπαϊκής Ένωσης, με ισχυρό αντίκτυπο στα δικαιώματα και τις ελευθερίες των ατόμων για τη θέσπιση κανόνων επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Σύμφωνα με τον GDPR, τα υποκείμενα των δεδομένων θα μπορούν (D. Hadjinestoros & Co LLC Publications):

1. Με την έννοια ότι μπορούν να γνωρίζουν τον σκοπό για τον οποίο θα χρησιμοποιηθούν τα δεδομένα από την αρχή, έχουν ευκολότερη πρόσβαση σε αυτά.
2. Θα έχουν το δικαίωμα να διαγράψουν τα δεδομένα που διατηρεί ένας υπεύθυνος επεξεργασίας δεδομένων. Το άρθρο 17 του GDPR ονομάζεται «δικαίωμα να λησμονηθεί» και στοχεύει να επιτρέψει στα άτομα να διαγράψουν τα δεδομένα τους χωρίς να επιθυμούν να επεξεργαστούν τέτοια δεδομένα (υπό την προϋπόθεση ότι δεν υπάρχουν νόμιμοι λόγοι για τον υπεύθυνο επεξεργασίας δεδομένων για να το διατηρήσει).
3. Σύμφωνα με το άρθρο 25 του κανονισμού, η προστασία δεδομένων περιλαμβάνεται από το σχεδιασμό και από προεπιλογή. Η προστασία δεδομένων από τη σχεδίαση σημαίνει ότι ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα για να ενσωματώσει τα απαραίτητα μέτρα προστασίας για την ικανοποίηση των απαιτήσεων του GDPR και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων. Προεπιλεγμένη προστασία δεδομένων σημαίνει ότι ο υπεύθυνος επεξεργασίας πρέπει να λάβει τα κατάλληλα μέτρα για να διασφαλίσει ότι μόνο τα προσωπικά δεδομένα που απαιτούνται για κάθε συγκεκριμένο σκοπό επεξεργασίας υποβάλλονται σε επεξεργασία από προεπιλογή, και δεν μπορούν να γίνουν προσβάσιμα, χωρίς την παρέμβαση του ατόμου.
4. Το άτομο έχει το δικαίωμα να γνωρίζει εάν και πότε έχει σημειωθεί παραβίαση ασφαλείας κάθε φορά που έχουν παραβιαστεί τα δεδομένα του. Ο GDPR δημιουργεί υποχρέωση στον υπεύθυνο επεξεργασίας δεδομένων όχι μόνο να ειδοποιεί την εποπτική αρχή για την παράβαση (και αυτό πρέπει να είναι εντός 72 ωρών), αλλά επίσης δημιουργεί την υποχρέωση κοινοποίησης στο υποκείμενο των δεδομένων προσωπική παραβίαση δεδομένων, περιγράφοντας τη φύση του την παραβίαση, καθώς και συστάσεις για το φυσικό πρόσωπο να μετριάσει τυχόν πιθανές δυσμενείς επιπτώσεις.

3.2 Δικαιώματα των ατόμων βάσει του GDPR

Υπάρχουν 99 διατάξεις, δικαιώματα και υποχρεώσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) (ReciprocityLabs, 2020). Ωστόσο, το GDPR παρέχει στα άτομα οκτώ (8) δικαιώματα σχετικά με τα προσωπικά τους δεδομένα. Αυτά τα δικαιώματα GDPR είναι δικαιώματα καταναλωτών και δικαιώματα εργαζομένων. Τα δικαιώματα των ατόμων βάσει του GDPR είναι τα εξής:

Δικαίωμα ενημέρωσης
Το GDPR δίνει στα άτομα το δικαίωμα να γνωρίζουν ότι τα προσωπικά τους δεδομένα συλλέγονται και πώς θα χρησιμοποιηθούν, πόσο καιρό θα διατηρηθούν και με ποιον θα μοιραστούν.

Δικαίωμα πρόσβασης
Το GDPR παραχωρεί σε άτομα ή "υποκείμενα δεδομένων" πρόσβαση στα δεδομένα που συλλέγονται σχετικά με αυτά. Πρέπει να παρέχετε αυτήν την πρόσβαση δωρεάν εντός ενός μηνός από τη λήψη του αιτήματος για προφορική ή γραπτή πρόσβαση στο υποκείμενο των δεδομένων.

Δικαίωμα διόρθωσης
Στις περισσότερες περιπτώσεις, τα υποκείμενα των δεδομένων μπορούν να διορθώσουν τα λάθη στα προσωπικά τους δεδομένα μέσα σε ένα μήνα μετά την υποβολή αιτήσεων για διορθώσεις προφορικά ή γραπτώς.

Δικαίωμα διαγραφής
Σε ορισμένες περιπτώσεις, τα υποκείμενα των δεδομένων ενδέχεται να διαγράψουν τα προσωπικά τους στοιχεία από αρχεία και συστήματα - αυτό είναι επίσης γνωστό ως "δικαίωμα λήψης" - για να ζητηθεί η διαγραφή προφορικά ή γραπτώς. Ομοίως, υπάρχει η διορία ενός μήνα για να απαντηθούν τα αιτήματά τους.

Δικαίωμα περιορισμού της επεξεργασίας
Εάν το υποκείμενο των δεδομένων ζητήσει τον περιορισμό ή την απαγόρευση των προσωπικών τους δεδομένων, σε ορισμένες περιπτώσεις πρέπει να συμμορφωθούν οι εταιρείες με τις επιθυμίες τους. Μπορούν να αποθηκεύσουν τα δεδομένα τους, αλλά μην χρησιμοποιηθούν.

Φορητότητα δεδομένων
Τα άτομα μπορούν να αποκτήσουν τα προσωπικά τους δεδομένα και να τα χρησιμοποιήσουν ξανά, να μετακινήσουν, να αντιγράψουν ή να τα μεταφέρουν από ένα μέρος σε άλλο.

Δικαίωμα αντίστασης
Τα άτομα ενδέχεται να αντιταχθούν στην επεξεργασία των προσωπικών σας δεδομένων και να απαγορεύσουν τη χρήση τους για άμεσο μάρκετινγκ - πρέπει να ενημερωθεί το υποκείμενο των δεδομένων για αυτό το δικαίωμα.

Δικαίωμα αυτόματης απόφασης και προφίλ
Το GDPR παρέχει στα άτομα συγκεκριμένα δικαιώματα στους ακόλουθους τομείς:

- Αυτοματοποιημένη λήψη αποφάσεων χωρίς χειροκίνητη παρέμβαση
- Αυτόματο προφίλ, όπου τα προσωπικά δεδομένα χρησιμοποιούνται για την αξιολόγηση διαφόρων πτυχών του υποκειμένου των δεδομένων

3.3 Συγκατάθεση Ενδιαφερομένων

Ένα από τα βασικά στοιχεία του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) είναι η συγκατάθεση των ενδιαφερομένων ως ένας τρόπος νομιμοποίησης του τρόπου επεξεργασίας των προσωπικών τους δεδομένων. Σύμφωνα με την αιτιολογική σκέψη 32, η συγκατάθεση δίνεται: «Με μια σαφή καταφατική πράξη που καθιερώνει μια ελεύθερα δοθείσα, συγκεκριμένη, ενημερωμένη και σαφή ένδειξη της συμφωνίας του υποκειμένου των δεδομένων για την επεξεργασία προσωπικών δεδομένων που σχετίζονται με αυτόν, όπως με γραπτή δήλωση, συμπεριλαμβανομένων με ηλεκτρονικά μέσα, ή προφορική δήλωση . Αυτό θα μπορούσε να περιλαμβάνει την επιλογή ενός πλαισίου όταν επισκέπτεστε έναν ιστότοπο διαδικτύου, την επιλογή τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας της πληροφορίας ή άλλη δήλωση ή συμπεριφορά που δείχνει σαφώς σε αυτό το πλαίσιο την αποδοχή του υποκειμένου των δεδομένων για την προτεινόμενη επεξεργασία των προσωπικών του δεδομένων. Η σιωπή, τα προεπιλεγμένα κουτιά ή η αδράνεια δεν πρέπει συνεπώς να αποτελούν συναίνεση. Η συγκατάθεση πρέπει να καλύπτει όλες τις δραστηριότητες επεξεργασίας που πραγματοποιούνται για τον ίδιο σκοπό ή σκοπούς. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δοθεί συγκατάθεση για όλους. "
Ένας τομέας στον οποίο η ενημερωμένη συγκατάθεση έχει ιδιαίτερη σημασία είναι η υγεία, καθώς λειτουργούν όχι μόνο με τυπικά προσωπικά δεδομένα, αλλά και με αυτά που είναι γνωστά ως ευαίσθητες πληροφορίες (Marovic and Curcin, 2020). Το άρθρο 9 του GDPR αντικατοπτρίζει την κύρια νομική βάση για την επεξεργασία τέτοιων δεδομένων (συγκατάθεση), η οποία θα πρέπει να είναι σαφής σύμφωνα με τους νέους ευρωπαϊκούς κανονισμούς. Τα νοσοκομεία και άλλα ιατρικά ιδρύματα πρέπει να κάνουν περισσότερα για να αποδείξουν ότι οι ασθενείς κατανοούν και αποδέχονται τους όρους χρήσης τους. Τα κέντρα που δεν έχουν τροποποιήσει τους όρους της συμφωνίας τους για να πληρούν τις απαιτήσεις πρέπει τώρα να επανεξετάσουν τις συμφωνίες τους για να λάβουν τη συγκατάθεση του ασθενούς.
Από την άλλη, οι διατάξεις του άρθρου 9 παράγραφος 2 ορίζουν τις ειδικές περιστάσεις υπό τις οποίες επιτρέπεται ή απαιτείται πραγματικά η επεξεργασία δεδομένων

(Ioannidou, 2019). Ανεξάρτητα από το εάν το υποκείμενο των δεδομένων συμφωνεί ή όχι, θα έχει σοβαρές επιπτώσεις στην ιατρική βιομηχανία. Οι επαγγελματίες του ιατρικού τομέα είναι συχνά σε θέση να αδυνατούν έναν ασθενή και δεν μπορούν να λάβουν τη συγκατάθεσή του. Μέσω αυτού του άρθρου, ο GDPR επιχειρεί να αντιμετωπίσει αυτήν την κατάσταση επιτρέποντας στους γιατρούς να αποκαλύψουν δεδομένα ασθενών σχετικά με την ανικανότητα των ασθενών, κάτι που είναι προς τα ζωτικά συμφέροντα των ασθενών.

3.4 Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ)

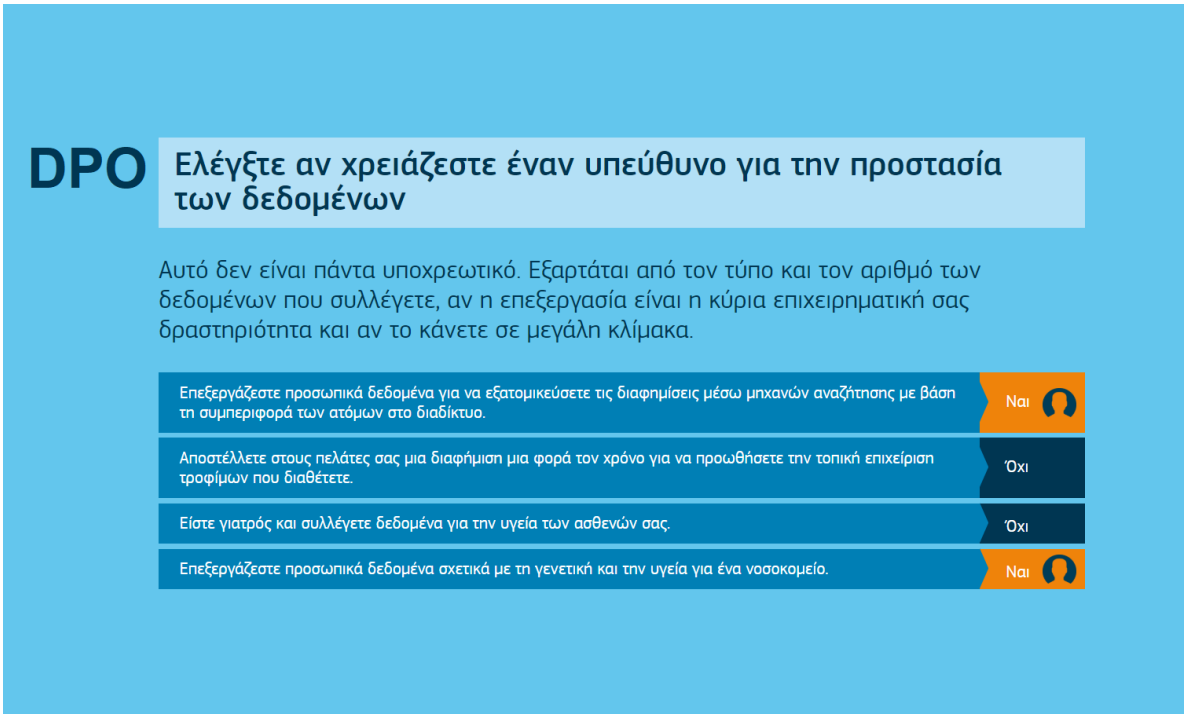
Σύμφωνα με τον GDPR, πρέπει να οριστεί ένας ΥΠΔ εάν:

- Είναι δημόσια αρχή (εκτός από τα δικαστήρια που ενεργούν υπό τη δικαστική τους ιδιότητα)
- Οι βασικές σας δραστηριότητες περιλαμβάνουν τακτική και συστηματική παρακολούθηση των ατόμων σε μεγάλη κλίμακα (για παράδειγμα, παρακολούθηση συμπεριφοράς στο διαδίκτυο) ή
- Οι βασικές σας δραστηριότητες περιλαμβάνουν επεξεργασία μεγάλης κλίμακας ειδικών κατηγοριών δεδομένων (η οποία περιλαμβάνει πληροφορίες σχετικά με την υγεία ενός ατόμου) ή δεδομένα σχετικά με ποινικές καταδίκες και αδικήματα.

Έτσι, οργανισμοί όπως οι ιατροί και οι οδοντιατρικές πρακτικές, άλλοι επαγγελματίες υγείας και φαρμακεία, και ιδιαίτερα εκείνοι που εκτελούν εργασία NHS, πιθανότατα θα πρέπει να διορίσουν έναν ΥΠΔ. Ο πρωταρχικός ρόλος του υπευθύνου προστασίας δεδομένων είναι να διασφαλίσει ότι ο οργανισμός του επεξεργάζεται τα προσωπικά δεδομένα του προσωπικού, των πελατών, των παροχών ή οποιουδήποτε άλλου ατόμου (αναφέρεται επίσης ως υποκείμενο δεδομένων) σύμφωνα με τους ισχύοντες κανόνες προστασίας δεδομένων (Βλ. εικόνα 2).

Τα θεσμικά όργανα της ΕΕ, ο ισχύων κανονισμός για την προστασία δεδομένων (κανονισμός (ΕΕ) 2018/1725) υποχρεώνει κάθε οργανισμό που επεξεργάζεται προσωπικά δεδομένα να ορίσει ΥΠΔ. Ο κανονισμός (ΕΕ) 2016/679, ο οποίος υποχρεώνει ορισμένους οργανισμούς σε χώρες της ΕΕ να διορίσουν ΥΠΔ, έχει εφαρμοστεί από τις 25 Μαΐου 2018.

Ο διορισμός ενός ΥΠΔ πρέπει φυσικά να βασίζεται στις προσωπικές και επαγγελματικές του ικανότητες, αλλά πρέπει να δοθεί ιδιαίτερη προσοχή στις γνώσεις του σχετικά με τον κανονισμό προστασίας δεδομένων. Επίσης πολύ σημαντικό είναι η πλήρης κατανόηση του τρόπου λειτουργίας του οργανισμού και οι ιδιαιτερότητες του.



Εικόνα 2. Πότε ένας οργανισμός χρειάζεται ένα DPO.

3.4.1 Θέση του DPO στο οργανόγραμμα

Ο DPO αποτελεί αναπόσπαστο μέρος του οργανισμού, με στόχο να διασφαλίσει τη συμμόρφωση. Ωστόσο, ο ΥΠΔ θα πρέπει να είναι σε θέση να εκτελεί τα καθήκοντά του ανεξάρτητα. Στα θεσμικά και λοιπά όργανα της ΕΕ, υπάρχουν ορισμένες εγγυήσεις που εγγυώνται αυτήν την ανεξαρτησία. Όπως για παράδειγμα οι κανόνες για τα όργανα και τους οργανισμούς της ΕΕ προβλέπουν ρητά ότι ο ΥΠΔ δεν θα λάβει οδηγίες σχετικά με την εκτέλεση των καθηκόντων του. Δεν πρέπει να υπάρχει σύγκρουση συμφερόντων μεταξύ των καθηκόντων του ατόμου ως DPO και των άλλων καθηκόντων της, εάν υπάρχουν. Για την αποφυγή συγκρούσεων, συνιστάται ο ΥΠΔ να μην είναι υπεύθυνος επεξεργασίας δραστηριοτήτων, ή υπεύθυνος ανθρωπίνου δυναμικού. Ο ΥΠΔ δεν πρέπει να είναι υπάλληλος με σύμβαση βραχείας ή σταθερής διάρκειας, δεν πρέπει να αναφέρει σε άμεσο προϊστάμενο (παρά ανώτατο διοικητικό συμβούλιο). Ο οργανισμός πρέπει να προσφέρει προσωπικό και πόρους για την υποστήριξη του DPO για την εκτέλεση των καθηκόντων της. Από αυτήν την άποψη, οι ΥΠΔ σε θεσμικά όργανα και οργανισμούς της ΕΕ μπορούν να αποσπαστούν από έναν βοηθό ή αναπληρωτή DPO και μπορούν να βασίζονται σε συντονιστές προστασίας δεδομένων (DPC) σε κάθε τμήμα του οργανισμού. Ο ΥΠΔ θα πρέπει να έχει την εξουσία να ερευνά. Στα θεσμικά όργανα και τους οργανισμούς της ΕΕ, για παράδειγμα, οι DPO έχουν άμεση πρόσβαση σε όλες τις διαδικασίες προσωπικών δεδομένων και επεξεργασίας δεδομένων.

Τα βασικά καθήκοντα του DPO είναι να βοηθά τον υπεύθυνο επεξεργασίας ή τον επεξεργαστή σε όλα τα θέματα που σχετίζονται με την προστασία των προσωπικών δεδομένων. Γενικότερα ο ΥΠΔ πρέπει να ενημερώνει τον υπεύθυνο επεξεργασίας ή τον επεξεργαστή, καθώς και τους υπαλλήλους τους, για τις υποχρεώσεις τους βάσει του

νόμου περί προστασίας δεδομένων. Πρέπει να παρακολουθεί τη συμμόρφωση του οργανισμού με όλη τη νομοθεσία σχετικά με την προστασία των δεδομένων, συμπεριλαμβανομένων των ελέγχων, των δραστηριοτήτων ευαισθητοποίησης καθώς και της κατάρτισης του προσωπικού που συμμετέχει στις διαδικασίες επεξεργασίας. Επίσης καθήκον του είναι να παρέχει συμβουλές, να ενημερώνει και να εκπαιδεύει το προσωπικό. Ενεργά ως σημείο επαφής για αιτήματα από ιδιώτες σχετικά με την επεξεργασία των προσωπικών τους δεδομένων και την άσκηση των δικαιωμάτων τους. Σε τέτοιες περιπτώσεις ο οργανισμός πρέπει να εμπλέκει τον DPO εγκαίρως. Ο υπεύθυνος DPO δεν πρέπει να λαμβάνει οδηγίες από τον υπεύθυνο επεξεργασίας ή τον επεξεργαστή για την άσκηση των καθηκόντων του. Ο ΥΠΔ αναφέρεται απευθείας στο υψηλότερο επίπεδο διαχείρισης του οργανισμού.
Όπως αντιλαμβανόμαστε ο ΥΠΔ είναι πολύ σημαντικός παράγοντα για τη σωστή λειτουργία ενός οργανισμού, όσο αφορά το κανονισμό προστασίας προσωπικών δεδομένων. Η παρουσία του σε ένα οργανισμό που χειρίζεται προσωπικά δεδομένα θεωρείτε πλέον απαραίτητη.

3.5 Παραβίαση GDPR

Εάν το Γραφείο του Επιτρόπου Πληροφοριών (ICO) απαιτείται να διερευνήσει τον οργανισμό για διάφορους λόγους, ο οργανισμός θα πρέπει να αναφέρει τα μέτρα που έχουν ληφθεί για να διασφαλιστεί η συμμόρφωση (Chilvers, 2018). Εάν προκύψει παραβίαση δεδομένων και μια εμπιστοσύνη δεν ακολουθεί το απαραίτητο πλαίσιο συμμόρφωσης, ο ICO θα υποχρεωθεί να εκδώσει πρόστιμο (Βλ. εικόνα 3).
Σύμφωνα με τον GDPR, το ανώτατο όριο για χαμηλότερο πρόστιμο βαθμίδας 2 είναι 8 εκατομμύρια ευρώ ή 2% του ετήσιου παγκόσμιου κύκλου εργασιών του οργανισμού, όποιο από τα δύο είναι υψηλότερο. Ή, εάν ο οργανισμός έχει αγνοήσει τον GDPR, μια υψηλότερη βαθμίδα θα μπορούσε να επιβάλει πρόστιμα έως και 20 εκατομμύρια ευρώ ή 4% του ετήσιου κύκλου εργασιών, όποιο από τα δύο είναι υψηλότερο. Αυτό καθιστά το GDPR έναν από τους πιο σημαντικούς κανονισμούς που πρέπει να ληφθούν υπόψη όταν οι εταιρείες επεξεργάζονται προσωπικά δεδομένα (D. Hadjinestoros & Co LLC Publications).
Γενικά, η παραβίαση των υποχρεώσεων του υπευθύνου επεξεργασίας ή του επεξεργαστή ή η μη κοινοποίηση της παραβίασης του ICO εντός 72 ωρών μπορεί να οδηγήσει σε χαμηλότερο επίπεδο προστίμων, ενώ οι παραβιάσεις των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων θα οδηγήσουν σε υψηλότερο επίπεδο προστίμων.

Εικόνα 3. Κόστος μη συμμόρφωσης του κανονισμού.

Κεφάλαιο 4

4.1 GDPR και Δεδομένα Υγείας

Το GDPR θεωρεί ότι τα δεδομένα υγείας είναι μια ειδική κατηγορία προσωπικών δεδομένων. Θεωρούνται ως ευαίσθητα δεδομένα και υπόκεινται σε ειδικούς όρους σχετικά με τη θεραπεία και την πρόσβαση τρίτων. Ο GDPR εισάγει χρήσιμα έναν ορισμό των δεδομένων υγείας και διευκρινίζει ότι καλύπτει "δεδομένα σχετικά με την υγεία, δηλαδή δεδομένα που σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, συμπεριλαμβανομένης της παροχής υπηρεσιών υγειονομικής περίθαλψης, οι οποίες αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας αυτού του ατόμου. Ο κανονισμός θεωρεί ότι τα δεδομένα υγείας μπορεί να περιλαμβάνουν πληροφορίες σχετικά με το άτομο που συλλέγεται κατά τη διάρκεια της εγγραφής ή παροχής υπηρεσιών υγειονομικής περίθαλψης, έναν αριθμό, ένα σύμβολο ή ένα συγκεκριμένο άτομο που έχει ανατεθεί σε ένα φυσικό πρόσωπο για να προσδιορίσει με μοναδικό τρόπο αυτό το άτομο για λόγους υγείας, πληροφορίες που προέρχονται από τη δοκιμή ή την εξέταση ενός μέρους του σώματος, συμπεριλαμβανομένων γενετικών δεδομένων και βιολογικών δειγμάτων ή οποιωνδήποτε πληροφοριών σχετικά με, για παράδειγμα, μια ασθένεια, κίνδυνο ασθένειας (δηλαδή δεδομένα σχετικά με τη δυνητική μελλοντική κατάσταση υγείας ενός ατόμου), αναπηρία, ιατρικό ιστορικό ή την κλινική θεραπεία της φυσιολογικής ή βιοϊατρικής κατάστασης ενός ατόμου ανεξάρτητου από την πηγή του. "

Υπάρχουν μερικές διαφορές μεταξύ του κανονισμού Directive 95/46/EC και του GDPR για τα δεδομένα υγείας (Whalen, 2017). Το Directive 95/46/EC περιλαμβάνει δεδομένα σχετικά με την υγεία και παρέχεται «υψηλότερο επίπεδο προστασίας». Υπάρχει γενική απαγόρευση επεξεργασίας χωρίς ρητή συγκατάθεση. Σε σύγκριση με τους προηγούμενους κανονισμούς για την προστασία των δεδομένων υγείας, ο GDPR έχει καταβάλει περισσότερες προσπάθειες για να ανταποκριθεί στις νέες απαιτήσεις της εποχής της ψηφιακής υγείας, οι οποίες μπορούν να βοηθήσουν στην ενίσχυση της προστασίας των δεδομένων υγείας σε ολόκληρη την ΕΕ (Yuan and Li, 2019). Το GDPR απαιτεί περισσότερες πληροφορίες όπως το αν μεταφερθούν τα δεδομένα, πόσο θα διατηρηθούν και αν χρησιμοποιείται το προφίλ.

Η Claire Williams, κύριος συνεργάτης της εθνικής νομικής εταιρείας Mills & Reeve LLP, δήλωσε : «Το GDPR θα επηρεάσει σχεδόν όλους τους οργανισμούς με επιχειρήσεις στην ΕΕ, αλλά οι οργανισμοί υγειονομικής περίθαλψης θα επηρεαστούν περισσότερο από τους περισσότερους. Τα δεδομένα ειδικής κατηγορίας, τα οποία περιλαμβάνουν πληροφορίες σχετικά με την υγεία και τη θεραπεία ενός ατόμου, μπορούν να υποβληθούν σε επεξεργασία μόνο βάσει αυστηρών κανόνων συμμόρφωσης. Οι διασφαλίσεις σχετικά με την ενημέρωση των ατόμων πλήρως, την κοινή χρήση δεδομένων με άλλους και τη διατήρηση των δεδομένων με ασφάλεια γίνεται όλο και πιο δύσκολη για εξαιρετικά ευαίσθητες πληροφορίες. Συγκεκριμένα ζητήματα πρόκειται να προκύψουν για τους

οργανισμούς υγειονομικής περίθαλψης καθώς ενημερώνουν τις πολιτικές και τις διαδικασίες τους σχετικά με τη συλλογή, αποθήκευση και χρήση δεδομένων ασθενών», (Sturman, 2020). Ο Andrew Earnshaw, εμπειρογνώμονας υγειονομικής περίθαλψης στην PA Consulting Group υπογραμμίζει περαιτέρω τις πολυπλοκότητες (και την ανάγκη) για αυξημένη ανταλλαγή δεδομένων σε ολόκληρο τον κλάδο. "Το GDPR έχει ενισχύσει τις βασικές πολυπλοκότητες της κοινής χρήσης δεδομένων σε ένα κοινόχρηστο αρχείο φροντίδας, ιδίως την έννοια και τους μηχανισμούς που αφορούν τη συγκατάθεση και τις εξαιρέσεις ανταλλαγής δεδομένων".
Το GDPR φαίνεται πολύ πιο κατάλληλο για να ανταποκριθεί στις προκλήσεις της προστασίας δεδομένων προσωπικής υγείας στην εποχή της ψηφιακής υγείας. Παρέχει στους ασθενείς μεγαλύτερα δικαιώματα και εξουσίες για τον έλεγχο και την κυριότητα των δεδομένων υγείας και επιχειρεί να αποσαφηνίσει τα δικαιώματα και την προστασία των δεδομένων προσωπικής υγείας σε ψηφιακές συναλλαγές υγειονομικής περίθαλψης. Το πιο σημαντικό, εισήγαγε νέα πρότυπα προστασίας δεδομένων υγείας και ενίσχυσε τις υποχρεώσεις των υπευθύνων επεξεργασίας δεδομένων και των επεξεργαστών στον τομέα της υγείας. Πιο συγκεκριμένα, ο GDPR θέτει τα υψηλότερα πρότυπα για πληροφορίες και εργασίες συναίνεσης. Όπως αναφέρεται στο άρθρο 7, είναι απαραίτητο να «ενημερώσουμε τους ασθενείς για τους πιθανούς κινδύνους της συλλογής δεδομένων σε σαφή και κατανοητή γλώσσα και σε σαφή και κατανοητή μορφή».

4.1.1 Τύποι Προσωπικών δεδομένων στον κλάδο της υγείας

Δεδομένα υγείας: Σύμφωνα με τον GDPR, τα «δεδομένα υγείας» ορίζονται ως «προσωπικά δεδομένα που σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, συμπεριλαμβανομένης της παροχής υπηρεσιών υγειονομικής περίθαλψης, οι οποίες αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του».

Γενετικά δεδομένα: Τα «γενετικά δεδομένα» ορίζονται από τον GDPR ως «προσωπικά δεδομένα που σχετίζονται με κληρονομικά ή αποκτηθέντα γενετικά χαρακτηριστικά ενός φυσικού προσώπου τα οποία δίνουν μοναδικές πληροφορίες σχετικά με τη φυσιολογία ή την υγεία αυτού του φυσικού προσώπου και που προκύπτουν, ιδίως, από μια ανάλυση ενός βιολογικό δείγμα από το φυσικό πρόσωπο. "

Βιομετρικά δεδομένα: Τα «βιομετρικά δεδομένα» είναι «προσωπικά δεδομένα που προκύπτουν από συγκεκριμένη τεχνική επεξεργασία που σχετίζεται με τα φυσικά, φυσιολογικά ή συμπεριφορικά χαρακτηριστικά ενός φυσικού προσώπου, τα οποία επιτρέπουν ή επιβεβαιώνουν τη μοναδική ταυτοποίηση αυτού του φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα».

Αυτοί οι τύποι προσωπικών δεδομένων υπόκεινται στα δικαιώματα που παραχωρούνται στους πολίτες / κατοίκους της ΕΕ από τον GDPR, όπως οι απαιτήσεις συναίνεσης, ο DPO είναι υπεύθυνος για την υποχρέωση απόδειξης και εξήγησης του τρόπου συλλογής / χρήσης δεδομένων και του δικαιώματος διαγραφής ασθενών (Vashkover, 2019). Ταξινομούνται ως ευαίσθητα προσωπικά δεδομένα, εκτός εάν ληφθεί ρητή συγκατάθεση ή πληρούνται πολύ ειδικοί όροι, διαφορετικά οι κανονισμοί απαγορεύουν γενικά οποιαδήποτε μορφή επεξεργασίας. Υπάρχουν μερικές εξαιρέσεις (Trend Micro, 2018). Η επεξεργασία μπορεί συνήθως να πραγματοποιηθεί για να εκτιμηθεί η ικανότητα εργασίας

στην απασχόληση, η διαχείριση συστημάτων και υπηρεσιών υγείας και πρόνοιας ή το δημόσιο συμφέρον.

Όπως περιγράφεται στο άρθρο 6 του GDPR, η επεξεργασία δεδομένων προσωπικού χαρακτήρα θεωρείται νόμιμη εάν (Rohatgi, 2019):

1. Το υποκείμενο των δεδομένων έχει συμφωνήσει.
2. Είναι απαραίτητο να εκτελεστεί η σύμβαση στην οποία συμμετέχει το υποκείμενο των δεδομένων
3. Είναι απαραίτητο να εκτελεστεί η νομική υποχρέωση
4. Είναι απαραίτητο να προστατεύονται τα ζωτικά συμφέροντα των υποκειμένων των δεδομένων ή άλλων φυσικών προσώπων
5. Είναι απαραίτητο να εκτελούνται καθήκοντα που εκτελούνται προς το δημόσιο συμφέρον
6. Είναι απαραίτητο για τους σκοπούς των νόμιμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος.

Γενικά, οι οργανισμοί υγειονομικής περίθαλψης που διαχειρίζονται δεδομένα υγείας αναλαμβάνουν υψηλότερο επίπεδο προστασίας από τα γενικά προσωπικά δεδομένα και διατηρούν «δεδομένα υγείας», «γενετικά δεδομένα» και «βιομετρικά δεδομένα» με υψηλότερο επίπεδο προστασίας. Ο GDPR απαγορεύει την επεξεργασία αυτών των μορφών δεδομένων υγείας εκτός εάν το υποκείμενο των δεδομένων πρέπει να έχει δώσει «ρητή συγκατάθεση» - "Η επεξεργασία είναι απαραίτητη για τους σκοπούς της προληπτικής ή επαγγελματικής ιατρικής, για την αξιολόγηση της ικανότητας εργασίας του εργαζομένου, της ιατρικής διάγνωσης, της παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή της διαχείρισης συστημάτων και υπηρεσιών υγείας ή κοινωνικής περίθαλψης…"

4.1.2 GDPR και NHS

Το GDPR είναι ένα σημαντικό ζήτημα για όλους τους οργανισμούς και η Εθνική Υπηρεσία Υγείας (NHS) δεν αποτελεί εξαίρεση (Sturman, 2020). Το NHS συμμορφώνεται ήδη με μια σειρά πρόσθετων κανονισμών και πολιτικών Διακυβέρνησης Πληροφοριών (IG) που υπήρχαν πολύ πριν από την εξέταση του GDPR - ορισμένοι από τους οποίους είναι πιο αυστηροί από τον GDPR.
Όλοι οι υπάλληλοι του NHS έχουν νόμιμο καθήκον εμπιστοσύνης να προστατεύουν προσωπικά στοιχεία που ενδέχεται να επικοινωνήσουν μαζί τους κατά τη διάρκεια της εργασίας τους (NHS England report, 2019). Αυτό δεν είναι μόνο απαίτηση της συμβατικής ευθύνης του, αλλά και απαίτηση κοινού δικαίου περί εμπιστοσύνης και νομοθεσίας περί προστασίας δεδομένων - ο Ευρωπαϊκός Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) και ο Νόμος Προστασίας Δεδομένων 2018 (DPA2018) που εφαρμόζει τον GDPR στο Ηνωμένο Βασίλειο.

4.2 Παραδείγματα GDP στην Ευρώπη

4.2.1 Γαλλία

Η επισκόπηση του γαλλικού συστήματος προστασίας δεδομένων παρέχει ένα καλό παράδειγμα των «περαιτέρω συνθηκών» που τα κράτη μέλη μπορούν να υιοθετήσουν όσον αφορά τα δεδομένα υγείας και την αλληλεπίδρασή του με τον GDPR (Behlow and Aumage, 2016).
Το Loi Informatique et Libertés 1978 (LIL), που διαχειρίζεται προσωπικά δεδομένα στη Γαλλία, δεν καθορίζει την έννοια των δεδομένων υγείας. Η Γαλλική Υπηρεσία Προστασίας Δεδομένων (CNIL) πιστεύει ότι οι πληροφορίες που καθορίζουν τη φύση μιας ασθένειας, αναπηρίας ή ανεπάρκειας μπορούν να θεωρηθούν δεδομένα υγείας.

Το LIL απαγορεύει την επεξεργασία δεδομένων υγείας εκτός εάν ισχύουν συγκεκριμένες εξαιρέσεις. Οι εξαιρέσεις περιλαμβάνουν:

1. Τη συλλογή της ρητής συγκατάθεσης του ατόμου (π.χ. απαιτείται ρητή συγκατάθεση από τον ασθενή για το άνοιγμα ενός φακέλου ιατρικού προσωπικού που είναι το Γαλλικό Προσωπικό Αρχείο Υγείας).
2. Επεξεργασία που είναι απαραίτητη για τους σκοπούς της προληπτικής ιατρικής, της ιατρικής διάγνωσης, της παροχής υγειονομικής περίθαλψης ή θεραπείας ή για τη διαχείριση των υπηρεσιών υγειονομικής περίθαλψης που πραγματοποιούνται από μέλος ιατρικού επαγγέλματος· στατιστική επεξεργασία που πραγματοποιείται από το Εθνικό Ινστιτούτο Στατιστικών και Οικονομικών Σπουδών (INSEE) ή απαραίτητη επεξεργασία για ιατρική έρευνα.

4.2.2 Σερβία

Η κουλτούρα προστασίας δεδομένων στη Σερβία είναι σχετικά νέα και έχει επηρεαστεί από το PDPA08 και το έργο του Επιτρόπου. Τώρα που η ευθυγράμμιση του GDPR βρίσκεται σε εξέλιξη, οι προηγούμενες εμπειρίες αξίζουν περαιτέρω εξέτασης. Οι παράγοντες που λειτουργούν την τελευταία δεκαετία εξακολουθούν να έχουν μεγάλη επιρροή. Η μετάβαση στο PDPA18 δίνει έμφαση στους ρόλους του DPO, της διοίκησης των οργανισμών υγειονομικής περίθαλψης και των δικαστηρίων (Marovic and Curcin, 2020).

Ο νόμος για τα δικαιώματα των ασθενών του 2013, όπως τροποποιήθηκε το 2019, ορίζει ρητά ότι:

- Όλοι οι εργαζόμενοι στον τομέα της υγείας και οι συνεργάτες τους πρέπει να διασφαλίζουν το απόρρητο των δεδομένων προσωπικού χαρακτήρα και υγείας.

- Ιδιαίτερα, τα ευαίσθητα δεδομένα πρέπει να αντιμετωπίζονται κατά τρόπο που να διασφαλίζει πάντοτε το απόρρητο και το απόρρητο
- Όλα τα ιδρύματα υγειονομικής περίθαλψης και άλλα νομικά πρόσωπα που χειρίζονται τέτοια δεδομένα είναι υποχρεωμένα να θεσπίζουν και να διατηρούν κατάλληλα συστήματα και μέτρα ασφαλείας.

Αυτή η πράξη υποχρεώνει ρητά τους εργαζομένους στον τομέα της υγειονομικής περίθαλψης και άλλους που επεξεργάζονται αυτά τα δεδομένα να διατηρήσουν το απόρρητο, εκτός εάν συναινέσει γραπτώς ο ασθενής ή ο νόμιμος εκπρόσωπος ή με δικαστική απόφαση.
Οι κύριοι τύποι επαναλαμβανόμενων περιστατικών που αντιμετωπίζει το Γραφείο Επιτρόπων είναι οι εξής:

- Ακατάλληλη απόρριψη και ακόμη και επαναχρησιμοποίηση χαρτιού με προσωπικά ή ιατρικά δεδομένα.
- Ακατάλληλη αποκάλυψη πληροφοριών σχετικά με την κατάσταση υγείας των διασημοτήτων χωρίς την κατάλληλη συγκατάθεση.
- Προσωπικά δεδομένα υγείας και αρχεία που διέρρευσαν στα μέσα ενημέρωσης για να ταπεινώσουν άτομα για πολιτικούς σκοπούς.

Η περίπτωση του κεντρικού Ολοκληρωμένου Συστήματος Πληροφοριών για την Υγεία (IHIS) που εφαρμόστηκε από το Υπουργείο Υγείας (Υπουργείο Υγείας): Μεταξύ του 2016 και του 2018, ο Επίτροπος εξέδωσε πολλές γνώμες, προειδοποιήσεις, συστάσεις και συμπεράσματα για διάφορα τεχνικά και νομικά ζητήματα, όπως σοβαρές αποτυχίες στην προστασία των προσωπικών δεδομένων που ενέχουν υψηλό κίνδυνο μη εξουσιοδοτημένης πρόσβασης και άλλων παραβιάσεων δικαιωμάτων μεγάλης κλίμακας.

Η μετάβαση στο GDPR μπορεί να έχει απροσδόκητες παρενέργειες. Στο νομικό σύστημα της Δημοκρατίας της Σερβίας, δεν υπάρχουν ειδικοί κανονισμοί σχετικά με τις υπηρεσίες cloud computing. Λόγω της κερδοσκοπικής φύσης του PDPA08 και των νομαρχιακών νόμων που σχετίζονται με τα δεδομένα υγείας, οι οργανισμοί διστάζουν να υιοθετήσουν αυτό το μοντέλο λογισμικού ως υπηρεσία και να αποθηκεύσουν τα δεδομένα τους στο cloud ή να αναθέσουν σε εξωτερικούς παροχείς υπηρεσιών. Αυτό είχε ως αποτέλεσμα τοπικές αναπτύξεις πληροφορικής που δημιούργησαν προβλήματα συντήρησης για τους οργανισμούς και τους πωλητές που συνεργάζονται με αυτούς τους οργανισμούς. Το PDPA18 και το GDPR έθεσαν μια διαφορετική γωνία στη σχέση των υπευθύνων επεξεργασίας δεδομένων και των επεξεργαστών και συχνά συζητούσαν δογματικά θέματα ιδιοκτησίας και διαχείρισης δεδομένων. Το PDPA18 έχει τη δυνατότητα να διευκολύνει την υιοθέτηση νέων τεχνικών λύσεων. Ωστόσο, οι οργανισμοί απαιτούν πρακτική καθοδήγηση, ιδίως για μικρούς παροχείς υπηρεσιών υγείας που συνήθως δεν διαθέτουν τους πόρους και την εμπειρογνωμοσύνη για την ανάπτυξη σχετικών πολιτικών και διαδικασιών, τη δημιουργία εταιρικών σχέσεων και την καθοδήγηση στην εφαρμογή.

4.2.3 Ηνωμένο Βασίλειο

Προς το παρόν, το Ηνωμένο Βασίλειο, παρά το Brexit παραμένει κράτος μέλος της ΕΕ και είναι νομικά υποχρεωμένοι να συμμορφωθούν με τον GDPR (Stockwell et al., 2018).
Το Κοινοβούλιο μπορεί, θεωρητικά, να μπορεί να τροποποιήσει τους νόμους μας για την προστασία δεδομένων μόλις το Ηνωμένο Βασίλειο αποχωρήσει από την ΕΕ. Ωστόσο, η κυβέρνηση δήλωσε ότι η συνεχής, αδιάλειπτη και ασφαλής ροή δεδομένων προσωπικού χαρακτήρα μεταξύ της ΕΕ και του ΗΒ είναι ζωτικής σημασίας, αναγνωρίζει ότι η νομοθεσία του Ηνωμένου Βασιλείου θα πρέπει να είναι ισοδύναμη με τη νομοθεσία της ΕΕ για την επίτευξη αυτού του στόχου και επιδιώκει να επιτύχει μια νέα συμφωνία προστασίας δεδομένων με την ΕΕ στο πλαίσιο των διαπραγματεύσεων για το Brexit.

Όσον αφορά τα δεδομένα υγείας, αυτά περιλαμβάνουν προσωπικά δεδομένα:

- τρίτων, τα οποία δεν θα ήταν λογικό να αποκαλυφθούν χωρίς τη συγκατάθεση του τρίτου μέρους
- η αποκάλυψη της οποίας θα προκαλούσε σοβαρή βλάβη στη σωματική ή ψυχική υγεία του υποκειμένου των δεδομένων (ή άλλου ατόμου)
- που αποκτήθηκε από ή παρέχεται από ένα παιδί με την προσδοκία ότι δεν θα αποκαλυφθεί σε έναν ενήλικα που κάνει SAR για λογαριασμό του

4.2.4 Ολλανδία

Η Ολλανδική Αρχή Προστασίας Δεδομένων, που ονομάζεται Autoriteit Persoonsgegevens (εφεξής "ολλανδική DPA"), επέβαλε πρόσφατα το πρώτο πρόστιμο GDPR ύψους 460.000 ευρώ, στο Ολλανδικό Νοσοκομείο Haga, επειδή δεν είχε επαρκή εσωτερική ασφάλεια των αρχείων ασθενών που συνιστά παραβίαση του άρθρου 32 του κανονισμού (Ioannidou, 2019). Σε αυτήν την περίπτωση, πριν επιβάλει πρόστιμο, η Ολλανδική DPA ξεκίνησε έρευνα επειδή πολλά μέλη του προσωπικού του Νοσοκομείου της Χάγης μπόρεσαν να λάβουν το ιατρικό αρχείο μιας ολλανδικής διασημότητας χωρίς τη συγκατάθεσή της και την έγκρισή της. Κατά τη διάρκεια της έρευνας, η Ολλανδική DPA έλεγξε εάν το σύστημα ασφάλειας πληροφοριών του νοσοκομείου συμμορφώνεται με τις απαιτήσεις ασφαλείας του άρθρου 32 των κανονισμών, ειδικά ορισμένα πρότυπα ιατρικής ασφάλειας. Το νοσοκομείο της Χάγης παρακολουθείται επί του παρόντος για να εξασφαλιστεί ότι η ασφάλειά του έχει βελτιωθεί. Εάν η ασφάλιση δεν πληροί τα πρότυπα που απαιτούνται από τον GDPR πριν από τις 2 Οκτωβρίου 2019, θα επιβάλλεται πρόστιμο 100.000 έως 300.000 ευρώ κάθε δύο εβδομάδες. Σύμφωνα με το GDPR, το νοσοκομείο Haga έπρεπε να είχε εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση ενός επιπέδου ασφάλειας κατάλληλου για τον κίνδυνο, και είχε το καθήκον να λάβει μέτρα για να διασφαλίσει ότι κάθε άτομο που ενεργεί υπό την εξουσία του και έχει πρόσβαση σε προσωπικά δεδομένα των ασθενών, δεν επεξεργάζεται τα δεδομένα αυτά εκτός από οδηγίες από το νοσοκομείο.

4.2.5 Πορτογαλία

Η Πορτογαλική Εποπτική Αρχή, που ονομάζεται Comissão Nacional de Protecção de Dados (από τώρα και στο εξής «CNPD»), στις 17 Ιουλίου 2018 επέβαλε πρόστιμο 400.000 ευρώ σε νοσοκομείο λόγω παραβίασης του GDPR (Ioannidou, 2019). Σύμφωνα με μια εφημερίδα, το CNPD διεξήγαγε έρευνα στο νοσοκομείο και διαπίστωσε ότι το προσωπικό του νοσοκομείου μπορούσε να έχει πρόσβαση σε δεδομένα ασθενών χρησιμοποιώντας ψευδή προσωπικά στοιχεία. Η έρευνα διαπίστωσε ότι το σύστημα διαχείρισης αρχείων φαίνεται να είναι ανεπαρκές, επειδή το νοσοκομείο σύμφωνα με πληροφορίες έχει μόνο 296 εγγεγραμμένους γιατρούς και υπάρχουν περίπου 985 αρχεία γιατρών στη βάση δεδομένων. Επίσης, η έρευνα διαπίστωσε ότι ανεξάρτητα από την ειδικότητα του γιατρού, είχε απεριόριστη πρόσβαση σε όλα τα αρχεία των ασθενών.

Σε αυτή τη βάση, το Εθνικό Λαϊκό Συνέδριο κατέληξε στο συμπέρασμα ότι υπάρχει σαφής παραβίαση του άρθρου 5 παράγραφος 1 στοιχείο γ) των κανονισμών, διότι πάρα πολλοί χρήστες μπορούν να χρησιμοποιήσουν τα προσωπικά δεδομένα που καταγράφονται από τους ασθενείς. Επιπλέον, διαπιστώθηκε επίσης ότι παραβιάστηκαν οι αρχές της ακεραιότητας και της εμπιστευτικότητας σύμφωνα με το άρθρο 5 παράγραφος 1 στοιχείο στ) των κανονισμών. Ως αποτέλεσμα της έρευνας του CNPD, συνήχθη το συμπέρασμα ότι το νοσοκομείο δεν εφάρμοσε τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτούνται για τη συμμόρφωση με τον GDPR (σχεδιασμένο για την προστασία των δεδομένων των ασθενών). Το νοσοκομείο προσπάθησε να δικαιολογήσει τις ενέργειές του με την υποδομή πληροφοριών που χρησιμοποιεί το πορτογαλικό Υπουργείο Υγείας για δημόσια νοσοκομεία. Ωστόσο, η CNPD αποφάσισε ότι το νοσοκομείο είναι υπεύθυνο για τη διασφάλιση της οργάνωσης και εφαρμογής κατάλληλων τεχνικών μέτρων για τη διασφάλιση της συμμόρφωσης με τον GDPR.

4.2.6 Γερμανία

Στο PegaWorld 2019, η γερμανική εταιρεία DAK Gesundheit συζήτησε πώς οι εκτιμήσεις του GDPR επηρέασαν την προσέγγισή τους στην αφοσίωση των πελατών προς έναν. Προκειμένου να συμμορφωθούν με τους νέους κανονισμούς, έχουν ενσωματώσει κανόνες και διαδικασίες αφοσίωσης πελατών που σχετίζονται με την επαφή, τα νομικά δικαιώματα και τη διαφήμιση (Rohatgi, 2019).

4.3 Το GDPR εκτός από την Ευρωπαϊκή Ένωση

Εκτός ΕΕ, υπάρχουν αυστηρές απαιτήσεις για τη διαβίβαση δεδομένων, η οποία απαιτεί άλλα προστατευτικά μέτρα. Για παράδειγμα, ένα προστατευτικό μέτρο επιτρέπει στην Ευρωπαϊκή Επιτροπή να καθορίσει εάν μια χώρα διαθέτει «επαρκές» επίπεδο προστασίας της ιδιωτικής ζωής των δεδομένων για τη μεταφορά δεδομένων σε αυτήν. Από τώρα και στο εξής, μια επαρκής διαδρομή θα είναι το GDPR (Privacy International, 2018). Τουλάχιστον μέχρι στιγμής, ο GDPR θα γίνει επίσης ένα από τα υψηλότερα (αν όχι τα υψηλότερα) ολοκληρωμένα πρότυπα προστασίας δεδομένων που είναι διαθέσιμα στον

κόσμο. Όταν άλλες χώρες υιοθετήσουν ή μεταρρυθμίσουν τα πλαίσια προστασίας δεδομένων τους, το GDPR θα γίνει το αδιαμφισβήτητο σημείο αναφοράς.

Το GDPR διαθέτει εισαγόμενα προϊόντα από την ιατρική βιομηχανία, κάτι που δεν είναι ξένο στους κανονισμούς σάρωσης. Στις Ηνωμένες Πολιτείες, οι περισσότεροι από αυτούς τους κανονισμούς περιλαμβάνονται ρητά στον Νόμο για τη φορητότητα και την ασφάλιση υγείας (HIPAA). Σημαντικές εκτιμήσεις περιλαμβάνουν τη ροή εργασίας δεδομένων, την επεξεργασία δεδομένων, τη διασυνοριακή μεταφορά δεδομένων, το απόρρητο των δεδομένων, την παρακολούθηση της ασφάλειας και τη συνολική συμμόρφωση με την πολιτική (Rohatgi, 2019).

Το GDPR είναι παρόμοιο με το HIPAA επειδή απαιτεί αυστηρά μέτρα ασφαλείας για τη ρύθμιση της χρήσης ιατρικής τεχνολογίας και κλινικών δεδομένων. Το αίτημα του GDPR να αναφέρει παραβίαση δεδομένων εντός 72 ωρών από την ανακάλυψη είναι διαφορετικό. Σύμφωνα με το HIPAA, οι παροχείς υγειονομικής περίθαλψης έχουν 60 ημέρες για να αναφέρουν παραβιάσεις. (Vashkover, 2019). Στις Ηνωμένες Πολιτείες, αποτελεί από καιρό κοινή πρακτική για τα ιατρικά ιδρύματα να διατηρούν επ' αόριστόν αρχεία των ασθενών. Ωστόσο, σύμφωνα με το GDPR, οι πολίτες της ΕΕ μπορούν να απαιτήσουν από τους παροχείς υγειονομικής περίθαλψης να διαγράψουν τα αρχεία τους υπό ορισμένες προϋποθέσεις.

Οργανισμοί σε όλο τον κόσμο που συνεργάζονται με πολίτες της ΕΕ πρέπει να ενημερώσουν τις πολιτικές διαχείρισης δεδομένων τους με διαφορετικούς τρόπους. Ακόμα και αν οι οργανισμοί συναλλάσσονται με πολίτες της ΕΕ από καιρό σε καιρό, η συμμόρφωση με τον GDPR εξακολουθεί να τους δίνει μια αρχή στη διαχείριση και προστασία δεδομένων. Πολλές χώρες και περιοχές ευθυγραμμίζονται με την ΕΕ και εφαρμόζουν ολοκληρωμένες πολιτικές ή τροποποιούν κανονισμούς για να συμμορφωθούν με τον GDPR (Trend Micro, 2018).

4.4 Εκπαίδευση Προσωπικού

Η εκπαίδευση και η κατάρτιση των εργαζομένων υγείας πρέπει να γίνει πιο εντατική, γιατί οι επαγγελματίες υγείας πρέπει να ενημερωθούν περαιτέρω για να εφαρμοστεί ο νέος κανονισμός (Yuan and Li, 2019). Γενικά, οι περισσότερες παραβιάσεις δεδομένων είναι εσωτερικές και όχι εξωτερικές. Η εσωτερική εκπαίδευση της προστασίας των δεδομένων είναι επομένως απαραίτητη για όλο το προσωπικό. Η ανεπαρκής εκπαίδευση μπορεί να οδηγήσει σε εσωτερική διαρροή δεδομένων, η οποία με τη σειρά της οδηγεί σε υψηλά πρόστιμα GDPR και τεράστιες οικονομικές απώλειες για τους παροχείς υγειονομικής περίθαλψης.

Είναι επίσης απαραίτητο να προσληφθούν άτομα που διαθέτουν τα κατάλληλα προσόντα για τους βασικούς ρόλους του GDPR, όπως αξιωματικοί προστασίας δεδομένων που αναλαμβάνουν την ενημέρωση, την παροχή συμβουλών και την παρακολούθηση της

συμμόρφωσης, τις ομάδες απορρήτου δεδομένων και τους διαχειριστές έργων και προγραμμάτων πληροφορικής. Για τους ψηφιακούς οργανισμούς υγειονομικής περίθαλψης των οποίων η κύρια δραστηριότητα είναι η ψηφιακή υγειονομική περίθαλψη, η έλλειψη τέτοιου προσωπικού αναμένεται να είναι ενοχλητική. Θα πρέπει να ενεργήσουν νωρίς για να αποτρέψουν τη σοβαρότερη έλλειψη προσωπικού που προκαλείται από τον ανταγωνισμό για ανθρώπινους πόρους κατά την εφαρμογή του GDPR.

4.4.1 Παραβίαση GDPR από εργαζομένους

Οι εργαζόμενοι άθελα τους μπορούν να παραβιάσουν τους κανόνες του GDPR. Σύμφωνα με το Appoint Recruitment (2019):

- Το 35% των ατόμων ανταποκρίνονται σε email εργασίας μέσω των προσωπικών τους κινητών τηλεφώνων μετά τη δουλειά.
- Το 25% το κάνει κατά τη διάρκεια των μεσημεριανών διαλειμμάτων και το 23% κατά τη μεταφορά.
- Παράλληλα, το 53% των «πρώτων εργαζομένων» χρησιμοποιούν το WhatsApp και άλλες εφαρμογές ανταλλαγής μηνυμάτων για λόγους εργασίας πολλές φορές την ημέρα. Τα 1/5 των τμημάτων ανθρώπινου δυναμικού δεν γνωρίζουν καν για αυτήν τη δραστηριότητα.
- Άλλοι (38%) χρησιμοποιούν ιστότοπους κοινωνικών μέσων για επικοινωνίες εργασίας.
- Μία από τις μεγαλύτερες ομάδες που αναφέρθηκαν, το 64% των ατόμων προωθούν τα email των πελατών ή των πελατών τους σε έναν προσωπικό λογαριασμό email.

Κεφάλαιο 5

5.1 Εισαγωγή

Αυτό το κεφάλαιο περιγράφει την ερευνητική μεθοδολογία της διατριβής. Πιο συγκεκριμένα, σε αυτό το κεφάλαιο ο συγγραφέας περιγράφει την ερευνητική στρατηγική που χρησιμοποιήθηκε. Την ερευνητική μέθοδο και την ερευνητική προσέγγιση, που χρησιμοποιήθηκε για τη συλλογή δεδομένων, την επιλογή δείγματος, την ερευνητική διαδικασία και τον τύπο της ανάλυσης δεδομένων. Αυτό το κεφάλαιο εξετάζει επίσης μια ηθική αντανάκλαση της διατριβής και των περιορισμών αυτής της έρευνας σχετικά με το υπό έρευνα αντικείμενο.

5.2 Ερευνητική στρατηγική

Η έρευνα που πραγματοποιήθηκε σε σχέση με αυτή τη διατριβή ήταν πολύ καινούργια. Προηγούμενη έρευνα δεν υπάρχει σχετικά την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων στο χώρο της υγείας, στην Κύπρο. Υπάρχει ένα μεγάλο κενό στην έρευνα στα τρέχοντα ακαδημαϊκά περιοδικά που αντιμετωπίζουν το ρόλο GDPR στο χώρο της υγείας. Αυτός είναι και ο κυριότερος λόγος που διεξάγει η ερεύνα.

5.3 Μέθοδος Έρευνας - Ποσοτική Τεχνική

Η ερευνητική μεθοδολογία ορίζεται από τους Leedy & Ormrod (2001, σελ. 14) ως «η γενική προσέγγιση που ακολουθεί ο ερευνητής κατά την εκτέλεση του ερευνητικού έργου». Οι ποσοτικές και ποιοτικές ερευνητικές μέθοδοι διερευνούν διαφορετικούς ισχυρισμούς στη γνώση και οι δύο μέθοδοι έχουν σχεδιαστεί για την επίλυση συγκεκριμένων τύπων ερευνητικών προβλημάτων (Williams, 2007). Οι ποσοτικές μέθοδοι παρέχουν ένα αντικειμενικό μέτρο της πραγματικότητας, ενώ οι ποιοτικές μέθοδοι επιτρέπουν στους ερευνητές να μελετήσουν καλύτερα και να κατανοήσουν την πολυπλοκότητα των φαινομένων. Η ποσοτική έρευνα περιλαμβάνει τη συλλογή δεδομένων έτσι ώστε οι πληροφορίες να μπορούν να ποσοτικοποιηθούν και να υποβληθούν σε στατιστική επεξεργασία προκειμένου να υποστηρίξουν ή να αντικρούσουν τους «εναλλακτικούς ισχυρισμούς γνώσης» (Creswell, 2003, σελ. 153). Η ποσοτική έρευνα υιοθετεί δομημένες διαδικασίες και επίσημα μέσα για τη συλλογή δεδομένων. Τα δεδομένα συλλέγονται αντικειμενικά και συστηματικά (Queirós et al., 2017).

Προκειμένου να επιτευχθούν οι σκοποί και οι στόχοι της διατριβής, πραγματοποιήθηκε ποσοτική έρευνα και συγκεκριμένα με την τεχνική της έρευνας και την βοήθεια ερωτηματολογίου. Μια έρευνα είναι μια ερευνητική τεχνική που επιτρέπει τη συλλογή δεδομένων απευθείας από άτομα που συμμετέχουν στον ερευνητή μέσω ενός συνόλου

ερωτήσεων που οργανώνονται με συγκεκριμένη σειρά (Queirós et al., 2017). Είναι μια από τις πιο ευρέως χρησιμοποιούμενες ποσοτικές τεχνικές, επειδή μπορεί να λάβει πληροφορίες σχετικά με ένα δεδομένο φαινόμενο ζητώντας ερωτήσεις που αντανακλούν τις απόψεις, τις απόψεις και τις συμπεριφορές μιας ομάδας ανθρώπων. Η έρευνα παρέχει πολλά οφέλη. Σε σύγκριση με άλλες εναλλακτικές λύσεις, τα δύο πιο σημαντικά οφέλη αυτής της μεθόδου είναι το υψηλό ποσοστό συμμετοχής του πληθυσμού και το χαμηλό κόστος της μεθόδου. Από την άλλη πλευρά, η αξιοπιστία των δεδομένων της έρευνας εξαρτάται σε μεγάλο βαθμό από τη δομή της έρευνας και την ακρίβεια των απαντήσεων που παρέχονται από τους ερωτηθέντες. Μερικά επιπρόσθετα οφέλη της έρευνας είναι ότι αποδοτική, είναι εύκολη η συλλογή και η ανάλυση των δεδομένων χρησιμοποιώντας στατιστικούς μεθόδους. Υπάρχει υψηλή αντιπροσωπευτικότητα και δεν επηρεάζεται από την υποκειμενικότητα του ερευνητή. Αντιθέτως, κάποια επιπρόσθετα ελαττώματα της συγκεκριμένης μεθόδου είναι η ακαμψία της δομής και δεν συλλαμβάνει συναισθήματα, συμπεριφορές και αλλαγές συναισθημάτων των ερωτηθέντων.

5.4 Μέθοδος και εργαλεία συλλογής δεδομένων

Για τους σκοπούς αυτής της έρευνας, χρησιμοποιήθηκε ένα δομημένο ερωτηματολόγιο (Παράρτημα 9.1) . Σκοπός του ερωτηματολογίου είναι η συλλογή πληροφοριών σχετικά με τον νέο κανονισμό και την εφαρμογή του στον τομέα της υγείας στην Κύπρο, η σύγκριση με άλλες χώρες και η ανάδειξη του επιπέδου της Κύπρου. Πραγματοποιήθηκε μια λίστα ερωτήσεων. Παρ' όλα αυτά ενδέχεται να απαιτηθούν πρόσθετες ερωτήσεις για να εξερευνήσουν τα ερευνητικά ερωτήματα και τους στόχους, δεδομένης της φύσης των γεγονότων σε συγκεκριμένους οργανισμούς υγείας. Η φύση των ερωτήσεων σημαίνουν ότι τα δεδομένα καταγράφηκαν με ακρίβεια και με σκοπό την επίτευξη του σκοπού και των στόχων της διατριβής.

Όσον αφορά τα εργαλεία συλλογής δεδομένων, η έρευνα περιλάβανε τη χρήση ερωτηματολογίων, η οποία χρησιμοποιήθηκε ως οδηγός συνάντησης για τον ερευνητή. Με το ερωτηματολόγιο δόθηκε και ένα φύλλο πληροφοριών συμμετεχόντων, το οποίο σκοπό είχε να ενημερώσει τους συμμετέχοντες για τη φύση της εργασίας. Με αυτό το φύλλο πληροφοριών είναι μια ένδειξη για τη συγκατάθεση των συμμετεχόντων στην συγκεκριμένη έρευνα (Παράρτημα 9.2). Το πλήρες φύλλο ερωτήσεων που χρησιμοποιήθηκε για την έρευνα βρίσκεται μετά το κεφάλαιο των Παραρτημάτων. Μερικά παραδείγματα των ερωτήσεων που περιλήφθηκαν στο ερωτηματολόγιο ήταν τα ακόλουθα:

1. Χειρίζεστε προσωπικά δεδομένα ασθενών ή προσωπικού της κλινικής σας;
2. Γνωρίζετε για το νέο κανονισμό προστασίας προσωπικών δεδομένων που εφαρμόστηκε το 2018;
3. Είχατε ενημέρωση για το νέο κανονισμό και τις αλλαγές που επιφέρει από τη διοίκηση του νοσοκομείου;

4. Από την εφαρμογή του κανονισμού και έπειτα θεωρείτε ότι άλλαξε κάτι στο τρόπο που εργάζεστε;
5. Από την εφαρμογή του κανονισμού και μέχρι σήμερα, άλλαξαν τα έντυπα ή/και κάποια ηλεκτρονικά αρχεία που χρησιμοποιούσατε;
6. Τι θα προτείνατε για καλύτερη εφαρμογή του κανονισμού στο νοσοκομείο που εργάζεστε;

5.5 Επιλογή δείγματος

Στην τρέχουσα μελέτη, τα μέλη του δείγματος που επιλέχθηκαν είχαν ειδική σχέση με το υπό εξέταση ζητούμενο, επαρκή και σχετική εργασιακή εμπειρία στον τομέα της υγειονομικής περίθαλψης και ενεργό συμμετοχή σε νοσοκομεία και κλινικές. Σε αυτό το πλαίσιο, οι συμμετέχοντες αυτής της μελέτης ήταν:

- Ιατρικό Προσωπικό
- Νοσηλευτικό Προσωπικό
- Άλλο παραϊατρικό Προσωπικό (Τεχνολόγοι, Φυσιοθεραπευτές, Λογοθεραπευτές, Εργοθεραπευτές, κ.α.)
- Γραμματειακό Προσωπικό
- Άλλο προσωπικό

5.6 Ερευνητική διαδικασία

Τα ερωτηματολόγια δόθηκαν στις αρχές Οκτωβρίου του 2020 στους συμμετέχοντες που αναφέρονται παραπάνω μέσω δημιουργίας φόρμας Google. Συγκεκριμένα, ο ερευνητής ήρθε σε επαφή μαζί τους μέσω email ή τηλεφωνικώς και τους ζήτησε να συμμετάσχουν στην έρευνα αφού τους εξηγήθηκε η φύση και το εύρος της μελέτης. Πριν αποσταλούν τα ερωτηματολόγια, ο ερευνητής ζήτησε άδεια από τα νοσοκομεία ή/και κλινικές, αφού οι συμμετέχοντες έπρεπε να παρέχουν εμπιστευτικές πληροφορίες. Σε γενικές γραμμές, οι ανταποκριτές ήταν πρόθυμοι να συμμετάσχουν στην έρευνα και τα ερωτηματολόγια απαντήθηκαν μέχρι τα μέσα Οκτωβρίου. Τα ερωτηματολόγια δόθηκαν στα ελληνικά για τη διευκόλυνση των ερωτηθέντων. Έχουν σταλεί συνολικά 150 ερωτηματολόγια και ανταποκρίθηκαν στα 74.

5.7 Ανάλυση δεδομένων

Η ανάλυση περιεχομένου χρησιμοποιήθηκε για την ανάλυση των δεδομένων που συγκεντρώθηκαν από τα ερωτηματολόγια. Όπως υποδεικνύουν οι Moore και McCabe (2005), αυτό είναι το είδος της έρευνας όπου οι πληροφορίες που συσσωρεύονται ταξινομούνται σε θέματα και υποκείμενα, προκειμένου να έχουν την ικανότητα να είναι παρόμοια. Μια αρχή ευνοϊκή θέση της ανάλυσης περιεχομένου είναι ότι βοηθάει στη μείωση και τη βελτίωση των πληροφοριών που συλλέγονται, ενώ παράλληλα δημιουργεί

αποτελέσματα που μπορεί στη συνέχεια να εκτιμηθούν χρησιμοποιώντας ποσοτικές μεθόδους. Επίσης, η ανάλυση περιεχομένου επιτρέπει στον ερευνητή να δομήσει τα ποσοτικά δεδομένα με τρόπο που να ικανοποιεί την επίτευξη των ερευνητικών προορισμών.

5.8 Ηθικά ζητήματα

Όλοι οι συμμετέχοντες ενημερώθηκαν για τις λεπτομέρειες της μελέτης μέσω ηλεκτρονικού ταχυδρομείου. Εκτός αυτού, τα μέλη ενημερώθηκαν πλήρως σχετικά με τους στόχους της έρευνας, ενώ ήταν σίγουροι ότι οι απαντήσεις τους αντιμετωπίζονταν ως ιδιωτικές και χρησιμοποιήθηκαν μόνο για επιστημονικούς σκοπούς και μόνο για τους λόγους της συγκεκριμένης έρευνας. Αλλά από τα παραπάνω, τα μέλη δεν πιέστηκαν να συμμετάσχουν, εν μέσω της διεξαγωγής της εξερεύνησης. Αντίθετα, ο ερευνητής προσπάθησε να δημιουργήσει και να διατηρήσει μια επαγγελματική ατμόσφαιρα.

5.9 Περιορισμοί έρευνας

Αυτή η διατριβή είχε διάφορους περιορισμούς, ειδικά για τον αριθμό των συμμετεχόντων που περιλαμβάνονται σε αυτήν την έρευνα. Άλλοι περιορισμοί είναι οι εξής:

- Το μέγεθος του δείγματος ήταν σχετικά μικρό - 74 συμμετέχοντες. Για τους σκοπούς της διατριβής έπρεπε να υπάρχει πλήρης αναλογία των οργανισμών που εμπίπτουν στα θέματα της υγείας στην Κύπρο, αλλά ήταν αδύνατο λόγω περιορισμού ανταπόκρισης από οργανισμούς, λαμβάνοντας υπόψη την πανδημία που ταλαιπωρεί τα νοσοκομεία και την υγειονομική περίθαλψη γενικότερα.
- Δεν ανταποκρίνονταν πολλοί οργανισμοί που ασχολούνται με την υγεία σε email και τηλεφωνικές κλήσεις.
- Σε ορισμένες περιπτώσεις οι συμμετέχοντες αρνήθηκαν να μιλήσουν εναντίον των οργανισμών τους, οπότε ο ερευνητής δεν γνωρίζει την αρνητική πλευρά.

5.10 Οργανισμοί υπό εξέταση

Επιλέχθηκε μια σειρά από διαφορετικά νοσοκομεία και κλινικές προκειμένου να εξεταστεί το θέμα της μελέτης σε μια ποικιλία πλαισίων. Οι συμμετέχοντες ήταν σε διάφορους ρόλους σε αυτούς τους οργανισμούς, προκειμένου να διερευνηθούν τα υπό μελέτη ζητήματα από διαφορετικές οπτικές γωνίες.

Το πρώτο νοσοκομείο υπό εξέταση ήταν το Mediterranean Hospital of Cyprus, στην Λεμεσό. Είναι ένα σύγχρονο ίδρυμα υγειονομικής περίθαλψης, ένα από τα μεγαλύτερα στην Κύπρο το οποίο είναι ιδιωτικό και προσφέρει υπηρεσίες του Γενικου Συστήματος Υγείας της Κύπρου. Το νοσοκομείο διαθέτει τμήμα έκτακτης ανάγκης, κλινικές εξωτερικών ασθενών σχεδόν όλων των ειδικοτήτων, τμήμα επεμβατικής και

νοσηλευτικής, χειρουργικό τμήμα καθώς ακτινολογικό και χημείο. Είναι πλήρως εξοπλισμένο και διαθέτει επαγγελματίες υγείας από διάφορες ειδικότητες.

Το δεύτερο υπό εξέταση ίδρυμα ήταν Μέλαθρον Αγωνιστών της ΕΟΚΑ. Ιατρικό Κέντρο, το οποίο περιλαμβάνει, Μονάδα Φυσικής Ιατρικής και Αποκατάστασης με 40 κλινες, Φυσιοθεραπευτήριο, Εξωτερικά Ιατρεία, Χημείο, Ακτινολογικό και Στέγη Ηλικιωμένων με 50 κλίνες. Ένα σύγχρονο ιατρικό κέντρο διαφορετικού χαρακτήρα από το προηγούμενο αφού έχει διαφορετική κατεύθηνση και αποστολή. Το κέντρο όμως έχει ένα μεγάλο αριθμό επαγγελματιών υγείας που έχουν καθημερινή επαφή με προσωπικά δεδομένα.

Το τρίτο υπό εξέταση ιατρείο είναι, ένα μικρό κέντρο υγείας στον Ύψωνα. Το ιατρείο αυτό είναι ένα μικρό ιατρείο, που προσφέρει υπηρεσίες του Γενικού συστήματος Υγείας της Κύπρου. Αποτελείτε από δύο προσωπικούς Γιατρούς (Παθολόγους), ένα Γενικό χειρούργο, ένα Ουρολόγο, δύο Ακτινολόγους, ένα Ορθοπεδικό και άλλους εξωτερικούς συνεργάτες. Το ιατρείο είναι εξοπλισμένο και με Ακτινολογικό Τμήμα το οποίο εξυπηρετεί ασθενείς της περιοχής και όχι μόνο. Στο ιατρείο αφού εργάζονται αρκετοί επαγγελματίες υγείας όπως γιατροί, νοσηλευτές, τεχνολόγοι ακτινολόγοι και γραμματειακό προσωπικό, όπως είναι λογικό χειρίζονται και προσωπικά δεδομένα ασθενών. Έτσι επιλέχθηκε για να συμπληρωθεί το ερωτηματολόγιο της έρευνας, μετά την επιλογή ενός μεγάλου κέντρου αποκατάστασης, μίας μεγάλης ιδιωτικής κλινικής, επιλέχθηκε και ένα μικρότερο ιατρείο με διάφορες υπηρεσίες, που εξυπηρετεί καθημερινά ένα μεγάλο αριθμό ασθενών.

Ο τέταρτος υπό εξέταση οργανισμός είναι Κέντρο Μαγνητικής Τομογραφίας Πάφου. Το Κέντρο Μαγνητικής Τομογραφίας Πάφου είναι ένα νέο διαγνωστικό κέντρο το οποίο προσφέρει ιατρικές διαγνωστικές υπηρεσίες όπως Μαγνητικό Τομογράφο και μηχάνημα (γ-camera). Το διαγνωστικό κέντρο Πάφου είναι ένα μικρό ακτινολογικό διαγνωστικό κέντρο, το οποίο προσφέρει τις υπηρεσίες του στο Γενικό Σύστημα Υγείας της Κύπρου. Στο κέντρο αυτό εργάζονται ιατροί Ακτινολόγοι, Αναισθησιολόγοι, Τεχνολόγοι Ακτινολόγοι καθώς και γραμματειακό προσωπικό. Όλοι αυτοί οι επαγγελματίες υγείας έρχονται σε καθημερινή επαφή με προσωπικά δεδομένα ασθενών. Επιλέχθηκε το κέντρο αυτό να συμμετέχει στην έρευνα γιατί είναι ένα μικρό Ακτινολογικό κέντρο, σε άλλη επαρχία και εξυπηρετεί καθημερινά μεγάλο αριθμό ασθενών.

Κεφάλαιο 6

Αποτελέσματα και Συζήτηση

6.1 Εισαγωγή

Αυτό το κεφάλαιο περιέχει τα κύρια ευρήματα μαζί με μια ανάλυση αυτών των ευρημάτων. Πιο συγκεκριμένα, σε αυτό το κεφάλαιο ο αναλυτής αναλύει τις απαντήσεις των ερωτηματολογίων ως προς έναν αριθμό θεμάτων που σχετίζονται με την ανασκόπηση της βιβλιογραφίας.

6.2 Προφίλ συμμετεχόντων

Οι ηλικίες των ερωτηθέντων κυμαίνονταν μεταξύ 20 ετών και άνω. Η πλειοψηφία (54,1%) των συμμετεχόντων ήταν μεταξύ 20 – 30 ετών. Το 17,6% των συμμετεχόντων ήταν μεταξύ 40 και 50 ετών, το 13,5% ήταν από 50 ετών και άνω και το 14,9% ήταν μεταξύ 30 και 40 ετών.

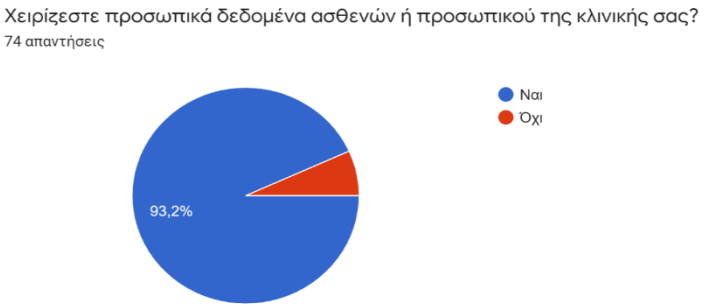
Για να παρθούν ανεξάρτητες και ποίκιλες απαντήσεις τα ερωτηματολόγια δόθηκαν σε διαφορετικούς οργανισμούς και τμήματα. Το 40,5% των συμμετεχόντων δουλεύει σε κέντρο αποκατάστασης, το 35,1% δουλεύει σε νοσοκομείο ή/ και κλινικές, το 23% δουλεύει σε ιατρείο (ιδιωτικό ιατρείο, οδοντιατρείο, κ.τ.λ) και το 1,4% δουλεύει σε ογκολογικό κέντρο. Το μεγαλύτερο ποσοστό των συμμετεχόντων (33.8%) δουλεύουν ως παραϊατρικό προσωπικό, όπως για παράδειγμα, τεχνολόγοι, φυσιοθεραπευτές, λογοθεραπευτές, εργοθεραπευτές, κ.τ.λ. Το 27% δουλεύει σαν γραμματειακό προσωπικό, το 18.9% δουλεύει σαν νοσηλευτικό προσωπικό, το 13,5% σαν ιατρικό προσωπικό και το υπόλοιπο 6,8% δουλεύει σε άλλα τμήματα των οργανισμών.

Θα πρέπει να σημειωθεί ότι στις απαντήσεις δεν αποτέλεσαν κριτήρια το φύλο, το επίπεδο εκπαίδευσης και τα έτη εργασιακής εμπειρίας των συμμετεχόντων. Οι πίνακες των αποτελεσμάτων μπορούν να βρεθούν αναλυτικότερα στο Παράρτημα 9.3.

6.3 Ανάλυση Αποτελεσμάτων και Συζήτηση

Η πρώτη ερώτηση που σχετίζεται με την έρευνα είναι αν οι εργαζόμενοι στα νοσοκομεία και κλινικές που συμπεριλαμβάνονται στην έρευνα χειρίζονται προσωπικά δεδομένα ασθενών ή προσωπικού της κλινικής που εργάζονται. Από τα αποτελέσματα φαίνεται ότι το 93,2% των ερωτηθέντων χειρίζονται προσωπικά δεδομένα (Βλ. Γράφημα 1). Από αυτά συμπεραίνουμε ότι ο Γενικός Κανονισμός Προσωπικών Δεδομένων είναι πολύ σημαντικός

για τον τομέα της υγείας αφού το μεγαλύτερο ποσοστό των εργαζομένων χειρίζονται ή επιβλέπουν προσωπικά δεδομένα.



Γράφημα 1: Αποτελέσματα Έρευνας για επεξεργασία προσωπικών δεδομένων.

Η επόμενη ερώτηση σχετίζεται με την πρώτη και ρωτά σε περίπτωση που χρησιμοποιούν ηλεκτρονικά αρχεία με προσωπικά δεδομένα, να επιλέξουν μια από τις παρακάτω απαντήσεις που εκφράζει καλύτερα την υφιστάμενη κατάσταση:

- Δεν χρησιμοποιώ κωδικούς, ανοίγοντας τον υπολογιστή βρίσκομαι στα αρχεία που χρειάζομαι
- Οι κωδικοί που χρησιμοποιώ είναι ατομικοί μου, δεν τους χρησιμοποιεί άλλος συνάδελφος και είναι ίδιοι εδώ και πολύ καιρό
- Οι κωδικοί που χρησιμοποιώ είναι ατομικοί μου, δεν τους χρησιμοποιεί άλλος συνάδελφος και αλλάζουν σε τακτά διαστήματα
- Οι κωδικοί που χρησιμοποιώ είναι κοινοί, τους χρησιμοποιούν και άλλοι συνάδελφοι και είναι ίδιοι εδώ και καιρό
- Οι κωδικοί που χρησιμοποιώ είναι κοινοί, τους χρησιμοποιούν και άλλοι συνάδελφοι και αλλάζουν σε τακτά διαστήματα

Η ερώτηση αυτή αποσκοπούσε στην συλλογή πληροφοριών που δείχνουν το πόσο βαθιά ή όχι έφτασε ο κανονισμός στο προσωπικό. Δηλαδή, θέλουμε να διαπιστωθεί το πόσο το προσωπικό είναι ενήμερο για το αν θα πρέπει να είναι περισσότερο επιφυλακτικό στην προστασία των προσωπικών δεδομένων και αν οι κωδικοί πρόσβασης μπορούν να θεωρηθούν ένα προστατευτικό μέσο.

Οι απαντήσεις που δόθηκαν υποδεικνύουν ότι περισσότεροι από τους μισούς συμμετέχοντες (52,9%) χρησιμοποιούν ατομικούς κωδικούς, που δεν χρησιμοποιεί άλλος συνάδελφός τους κα είναι ίδιοι εδώ και πολύ καιρό. Το μικρότερο ποσοστό (4,2%) από τους συμμετέχοντες χρησιμοποιούν κοινούς κωδικούς, που χρησιμοποιούν και άλλοι συνάδελφοι και αλλάζουν σε τακτά διαστήματα. Ένα σημαντικό ποσοστό (25,7%) λέει ότι οι κωδικοί που χρησιμοποιεί είναι κοινοί και χρησιμοποιούνται από άλλους συναδέλφους και δεν αλλάζουν σε τακτά διαστήματα. Αυτό έχει ως αποτέλεσμα την άμεση έκθεση των προσωπικών δεδομένων διαφορών τμημάτων του οργανισμού που

δεν συνάδει με τον Γενικό Κανονισμό Προσωπικών Δεδομένων και με το ιατρικό απόρρητο.

Μέσα από τα αποτελέσματα, συμπεραίνουμε ότι η πλειοψηφία των οργανισμών έχουν εφαρμόσει ατομικούς λογαριασμούς για το κάθε προσωπικό αλλά δεν ενημερώνονται και δεν αλλάζονται σε τακτά χρονικά διαστήματα. Με αυτό τον τρόπο είναι πολύ εύκολη η ηλεκτρονική απάτη και πολύ εύκολη η πρόσβαση σε προσωπικά δεδομένα.

Η επόμενη ερώτηση υποδεικνύει ότι το 71,6% των συμμετεχόντων γνωρίζουν για το νέο κανονισμό προστασίας προσωπικών δεδομένων που εφαρμόστηκε το 2018. Από ότι συμπεραίνουμε, ενώ το 93,2% χειρίζονται προσωπικά δεδομένα, το 28,4% από αυτούς δεν γνωρίζουν για το νέο κανονισμό. Στη συνέχεια, ρωτήθηκε στους συμμετέχοντες αν είχαν ενημέρωση για τον νέο κανονισμό από τη διοίκηση του νοσοκομείου και οι απαντήσεις ήταν σχεδόν μοιρασμένες στη μέση με το 52,7% να λέει ότι είχαν ενημέρωση από το νοσοκομείο(Βλ. Γράφημα 2). Αυτό το αποτέλεσμα δείχνει ότι υπάρχει μια μικρή απόκλιση από την προηγούμενη απάντηση όπου έδειξε μεγαλύτερο ποσοστό γνωρίζει για τον νέο κανονισμό. Συμπερασματικά, δείχνει ότι οι συμμετέχοντες μπορεί να γνωρίζουν για τον κανονισμό από εξωτερικές πηγές αλλά όχι από το νοσοκομείο. Επίσης, ένα άλλο συμπέρασμα από αυτήν την ερώτηση είναι ότι ένα μέρος ευθύνης για την άγνοια του προσωπικού για τον νέο κανονισμό να καταλογίζεται στις διοικήσεις των οργανισμών, για την έλλειψη ενημέρωσης. Από τα άτομα που έτυχαν ενημέρωση από τη διοίκηση του νοσοκομείου, το 25,7% έτυχε ενημέρωση με email, το 23% έτυχε ενημέρωση με σεμινάριο και το 5,4% έτυχε ενημέρωση με τμηματική ενημέρωση από τον υπεύθυνο τμήματος τους.

Γράφημα 2: Αποτελέσματα έρευνας για τυχόν ενημέρωση για το νέο κανονισμό.

Από την εφαρμογή του κανονισμού το 56,8% των συμμετεχόντων θεωρεί ότι δεν άλλαξε κάτι στον τρόπο που εργάζεται ενώ αυτό υποδηλώνει ότι οι οργανισμοί δεν άλλαξαν τις διαδικασίες τους ώστε να εφαρμόζεται σωστά και λειτουργικά ο κανονισμός. Από το 43,2% που απάντησε θετικά στην αλλαγή των εργασιών τους μετά τον κανονισμό, το 35,1% απάντησε ότι γίνεται καλύτερη προστασία δεδομένων, το 13,5% απάντησε ότι υπάρχει αυξημένος φόρτος εργασίας, το 10,8% απάντησε ότι γίνεται καλύτερη οργάνωση και το 1,4% απάντησε ότι υπάρχει μειωμένη παραγωγικότητα. Με τις πιο πάνω

απαντήσεις οδηγούμαστε στο συμπέρασμα ότι οι οργανισμοί έκαναν ελάχιστες αλλαγές σε διαδικασίες και έντυπα.

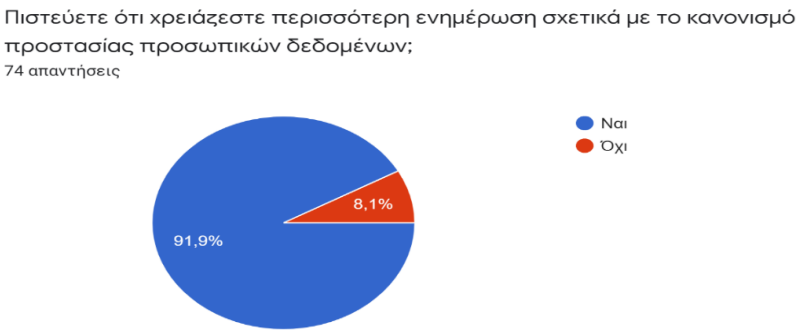
Από την εφαρμογή του κανονισμού το 2018 και μέχρι και σήμερα δεν έχουν αλλάξει τα έντυπα η/και τα ηλεκτρονικά αρχεία που χρησιμοποιούσαν το προσωπικό με το 58,1% να απαντά αρνητικά σε αυτή την αλλαγή. Το ερωτηματολόγιο συνεχίζεται με δύο αλληλένδετες ερωτήσεις που αφορούν το επίπεδο εφαρμογής του κανονισμού στους εκάστοτε οργανισμούς. Οι απαντήσεις ποικίλουν. Το 14,9% απάντησε ότι δεν εφαρμόζεται καθόλου ικανοποιητικά ο κανονισμός στον οργανισμό όπου δουλεύουν ενώ το 10,8% απάντησε ότι εφαρμόζεται πλήρως ικανοποιητικά. Οι απαντήσεις αυτές ίσως επηρεάζονται και από συναισθηματικό παράγοντα όπου οι συμμετέχοντες απάντησαν με το πόσο τους αρέσει ο οργανισμό όπου δουλεύουν ή αντιθέτως, με το πόσο δυσαρεστημένοι είναι από τον οργανισμό τους. Τα μεγαλύτερα ποσοστά συναντιούνται στη μέση όπου, ο κανονισμός εφαρμόζεται μερικώς. Η επόμενη ερώτηση για το επίπεδο του οργανισμού στην εφαρμογή του κανονισμού, αφορά τα περιθώρια βελτίωσης για τον κάθε οργανισμό με το 97,3% να απαντά ότι ο οργανισμός χρίζει σημεία βελτίωσης (Βλ. Γράφημα 3). Από την ερώτηση αυτή απορρέει το συμπέρασμα ότι σύμφωνα με το προσωπικό τους, όλοι οι οργανισμοί μπορούν να βελτιωθούν ως προς τον κανονισμό.

Γράφημα 3: Αποτελέσματα έρευνας για τα περιθώρια βελτίωσης των οργανισμών.

Για το νέο κανονισμό πρέπει να υπάρχει υποχρεωτικά το εγχειρίδιο πολιτικών, διαδικασιών και εγγράφων για τη σωστή επεξεργασία προσωπικών δεδομένων. Για τους ερωτηθέντες οργανισμούς το 59,5% απάντησε αρνητικά στην ύπαρξη του παραπάνω εγχειριδίου και το 40,5% απάντησε θετικά. Αυτή η ερώτηση είναι μία από αυτές που μπορεί να επιδείξει πόσο βαθιά ή όχι έφτασε ο κανονισμός στο προσωπικό ή όχι με τις απαντήσεις να είναι μοιρασμένες.

Όπως συμπεραίνουμε και από την επόμενη ερώτηση, στους οργανισμούς υγείας, χρειάζονται περισσότερη ενημέρωση σχετικά με τον κανονισμό προστασίας προσωπικών δεδομένων με το 91,9% να απαντά θετικά (Βλ. Γράφημα 4). Σε επόμενη ερώτηση η οποία ήταν ανοικτή και αφορά τρόπους και εισηγήσεις για καλύτερη εφαρμογή του κανονισμού στους οργανισμούς. Την ερώτηση αυτή την απάντησαν περίπου το 21% των συμμετεχόντων και όλοι αναφέρουν καλύτερη ενημέρωση από τη διοίκηση είτε

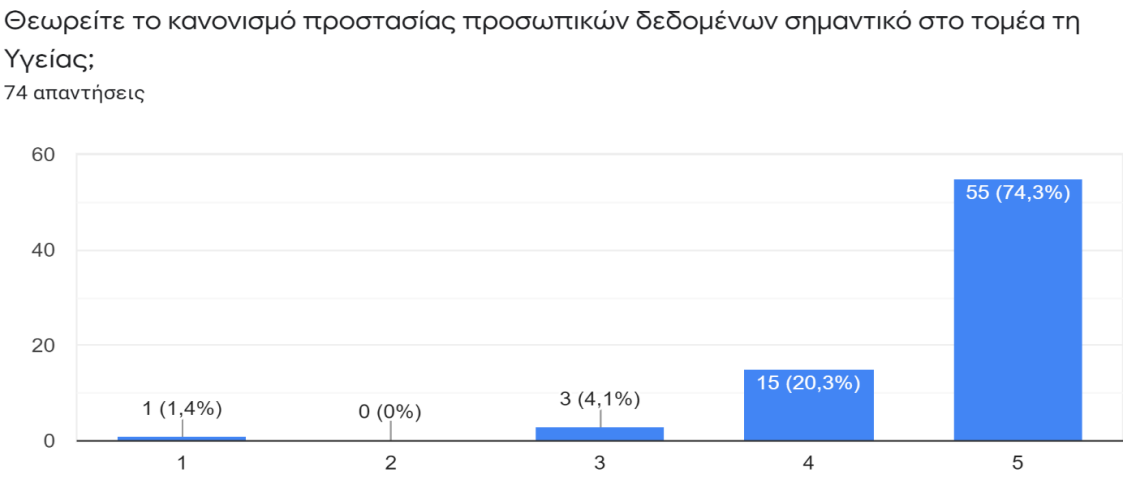
τμηματική είτε με σεμινάρια με τις περισσότερες εισηγήσεις να είναι καλύτερη ενημέρωση από τη διοίκηση με σεμινάριο.



Γράφημα 4: Αποτελέσματα έρευνας για περαιτέρω ενημέρωση σχετικά με το κανονισμό.

Τα δικαιώματα των εργαζομένων, μεταξύ άλλων, συμπεριλαμβάνουν και το δικαίωμα να μπορούν να βλέπουν αρχεία ασθενών άλλου γιατρού όταν υπάρχει μεγίστη ανάγκη. Ένα παράδειγμα είναι όταν το προσωπικό ενός ογκολογικού κέντρου, μπορεί να έχει πρόσβαση στο αρχείο υγείας ενός ασθενούς, που δεν είναι εξ ολοκλήρου δικός του ασθενής αλλά είναι μεγίστη ανάγκη να έχει πρόσβαση όταν δεν μπορεί να επικοινωνήσει μαζί με τον προσωπικό γιατρό τη συγκεκριμένη στιγμή. Μέσα από αυτή την έρευνα δείχνει ότι μόνο το 10,8% γνωρίζει πλήρως τα δικαιώματά τους που απορρέουν από τον Κανονισμό ενώ το 40,5% δεν γνωρίζει καθόλου τα δικαιώματα τους.

Τέλος, το μεγαλύτερο ποσοστό των συμμετεχόντων (74,3 %) απάντησε ότι είναι πολύ σημαντικός ο νέος κανονισμός προστασίας προσωπικών δεδομένων στο τομέα της υγείας και το 4,1% θεωρεί ότι ούτε σημαντικό αλλά ούτε και ασήμαντος είναι ο καινούργιος αυτός κανονισμός (Βλ. Γράφημα 5).



Γράφημα 5: Αποτελέσματα έρευνας για το πόσο σημαντικό θεωρεί τον κανονισμό ο πληθυσμός.

6.4 Σύγκριση Αποτελεσμάτων

Παρόμοια έρευνα έγινε για τους παροχείς υπηρεσιών υγείας στην Αθήνα, στην οποία οι ερευνητές κατέληξαν σε παρόμοια συμπεράσματα (Markopoulou et al., 2020). Το δείγμα της μελέτης αποτελούνταν από 229 νοσοκόμες (79,9% γυναίκες) με μέσο όρο ηλικίας 36,41 ετών. Η πλειονότητα των συμμετεχόντων (56,3%) εργάστηκε σε δημόσιο οργανισμό υγειονομικής περίθαλψης. Παρόλο που το 74,1% των συμμετεχόντων είχε ήδη ενημερωθεί για το GDPR, μόνο το 54,1% από αυτούς είχαν ενημερωθεί επίσημα στο χώρο εργασίας τους από τον οργανισμό τους. Συγκριτικά, η παραπάνω εργασία έχει σχεδόν τα ίδια ποσοστά στις ίδιες ερωτήσεις με την παρούσα εργασία. Στην συγκριτική εργασία το ποσοστό των εργαζόμενα που έχουν ενημερωθεί για τον κανονισμό είναι 74,1%, ενώ στην παρούσα εργασία είναι 71,6%. Επίσης, 54,1% από αυτούς έχουν ενημερωθεί από το χώρο εργασίας τους ενώ στην παρούσα εργασία το 52,7%.

Οι συμμετέχοντες στην συγκριτική εργασία ενημερώθηκαν επίσημα για το GDPR μέσω πολλαπλών πηγών: φυλλάδιο (54,0%), από τον επόπτη τους (40,3%), από τον ΥΠΔ (13,7%), ενώ στην παρούσα εργασία η ενημέρωση έγινε από email (25,7%) και από σεμινάριο (23%).

Όσον αφορά τη σύγκριση μεταξύ των δημογραφικών / επαγγελματικών χαρακτηριστικών των προηγούμενων ενημερωμένων συμμετεχόντων σχετικά με τον GDPR στο χώρο εργασίας τους, διαπιστώθηκε ότι στην συγκριτική έρευνα, οι προηγούμενοι ενημερωμένοι συμμετέχοντες διέφεραν σημαντικά ανάλογα με την ηλικία, το επίπεδο εκπαίδευσης, τον τύπο του τομέα της υγείας (δημόσιο / ιδιωτικό), τη θέση ευθύνης και τα έτη εργασιακής εμπειρίας. Στην παρούσα έρευνα δεν έπαιξε καθόλου ρόλο τα δημογραφικά και επαγγελματικά χαρακτηριστικά των ερωτηθέντων.

Οι δύο έρευνες έδειξαν ότι τόσο στην Κύπρο, όσο και στην Ελλάδα, υπάρχει έλλειψη πληροφόρησης θα μπορούσε να οδηγήσει σε σημαντικά πρόστιμα κατά των υπηρεσιών υγειονομικής περίθαλψης των συμμετεχόντων, λόγω της εσφαλμένης επεξεργασίας των ευαίσθητων προσωπικών δεδομένων των ασθενών.

Μια άλλη έρευνα που εξετάστηκε για σύγκριση είναι για τα κολλέγια που ασχολούνται με την υγεία (Wallace and Greene, 2019). Από τα 12 κολέγια που ήρθαν σε επαφή, τέσσερα ήταν ευχάριστα για τη διανομή της έρευνας. Το Κολλέγιο Ψυχιάτρων, το Κολλέγιο Οφθαλμολογίας και η Σχολή Ακτινολογίας έστειλαν την έρευνα μέσω email σε NCHDs στις λίστες αλληλογραφίας τους. Το Royal College of Physicians συμπεριέλαβε την έρευνα στο περιοδικό συνδρομητών email τους (e-zine). Ο τελικός πληθυσμός της μελέτης ήταν ένα δείγμα ευκολίας 192 NCHDs. Λόγω της μεθόδου διανομής, δεν κατάφεραν να υπολογίσουν το ποσοστό συμμετοχής. Ωστόσο, υπάρχουν περισσότερα από 7000 NCHDs εγγεγραμμένα στο Ιρλανδικό Ιατρικό Συμβούλιο. Επομένως, συνέλλεξαν απαντήσεις από

ένα πολύ μικρό δείγμα του πληθυσμού-στόχου. Ένα από τα συμπεράσματα της έρευνας είναι ότι απαιτείται ειδική εκπαίδευση και καθοδήγηση σε σχέση με το GDPR και το HRR σε εθνικό επίπεδο για να επιτρέψουν στους NCHD να συνεχίσουν με βεβαιότητα τη διεξαγωγή έρευνας. Οι εθνικοί φορείς υγείας, κατάρτισης και κυβερνήσεων πρέπει να γνωρίζουν τις πιθανές συνέπειες στα ποσοστά μετανάστευσης ως έμμεσο αποτέλεσμα αυτών των νέων κανονισμών και των επιπτώσεων στην εξέλιξη της σταδιοδρομίας. Απαιτείται περαιτέρω έρευνα σχετικά με την προσαρμογή της Ιρλανδικής NCHD σε αυτούς τους νέους κανονισμούς και τις επακόλουθες συνέπειες.

Όπως και στην παρούσα έρευνα, αποδείχτηκε ότι οι ο χώρος της υγείας χρειάζεται ειδική εκπαίδευση του προσωπικού για την σωστή και αποτελεσματική εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων. Είναι ανησυχητικό ότι μόνο το 25% των ερωτηθέντων στην Ιρλανδία έχουν εκπαιδευτεί σε αυτούς τους νέους κανονισμούς, σχεδόν δύο χρόνια μετά την εισαγωγή τους.

Κεφάλαιο 7

Συμπεράσματα

Φτάνοντας στο τέλος αυτής της ερευνητικής εργασίας μέσα από την βιβλιογραφική ανασκόπηση αλλά και από την έρευνα που πραγματοποιήθηκε εξάχθηκαν σημαντικά συμπεράσματα. Τα συμπεράσματα αφορούν τον Κανονισμό Προστασίας Προσωπικών Δεδομένων και την εφαρμογή του σε χώρους υγείας, καθώς και το επίπεδο που εφαρμόζεται στους τέσσερις οργανισμούς που ερευνήθηκαν.

Αρχικά να αναφερθεί ότι σύμφωνα με τα όσα μελετήθηκαν πιο πάνω για το σωστό σχεδιασμό ενός συστήματος προστασίας προσωπικών δεδομένων πρέπει να γίνει συνεργασία όλων των υπαλλήλων του οργανισμού. Πρώτο βήμα η σωστή επιλογή ενός ΥΠΔ που θα έχει γνώσεις και θα μπορεί να οδηγήσει τον οργανισμό σε πλήρη εναρμόνιση με τον κανονισμό. Ο ΥΠΔ είναι πολύ σημαντική θέση όσο αφορά τον κανονισμό προστασίας προσωπικών δεδομένων. Πρέπει να μελετήσει και να εισηγηθεί αλλαγές στο τρόπο λειτουργίας του οργανισμού για να εφαρμόζει τον κανονισμό. Όπως για παράδειγμα την αλλαγή των αρχείων και των εγγράφων που χρησιμοποιούνται, την σωστή καταστροφή των αρχείων κ.α. Να εφαρμοστούν μέθοδοι προστασίας των προσωπικών δεδομένων, όπως η επαλήθευση ταυτότητας με κωδικούς και η συχνή αλλαγή τους, η κρυπτογράφηση, η κάλυψη δεδομένων και η συγκατάθεση για επεξεργασία προσωπικών δεδομένων. Όλα αυτά για να υλοποιηθούν πρέπει να υπάρχει μια συνεργασία από την ομάδα του ΥΠΔ, της διοίκησης, του τμήματος πληροφορικής αλλά και των επαγγελματιών υγείας που θα κάνουν χρήση όλων αυτών.

Πολύ σημαντικό, είναι η ενημέρωση των υπαλλήλων του οργανισμού, σχετικά με τον κανονισμό. Αν εφαρμοστούν όλα όσα αναφέρθηκαν αλλά οι υπάλληλοι του οργανισμού δεν ενημερωθούν και εκπαιδευτούν σωστά πως να χειρίζονται τα προσωπικά δεδομένα, δεν θα επιτευχθεί τίποτα.

Όπως προέκυψε και από την έρευνα που διεξάχθηκε, οι οργανισμοί που ερευνήθηκαν δεν έχουν ενημερώσει το προσωπικό τους επαρκώς. Όλοι οι επαγγελματίες υγείας θεωρούν το κανονισμό αρκετά σημαντικό αλλά θεωρούν ότι χρειάζονται και περισσότερη ενημέρωση σχετικά με αυτόν. Επίσης σχεδόν όλοι οι επαγγελματίες στο χώρο της υγείας, έρχονται σε επαφή με προσωπικά δεδομένα ασθενών και θεωρούν ότι οι οργανισμοί υγείας χρίζουν βελτίωση ως προς το κανονισμό.

Συνοπτικά μπορούμε να πούμε ότι για το σχεδιασμό ενός σωστού προγράμματος με σκοπό την εφαρμογή του κανονισμού προστασίας προσωπικών δεδομένων είναι πολύ σημαντική η συνεργασία όλου του προσωπικού. Πολύ σημαντική η θέση του ΥΠΔ, ενός καλά οργανωμένου τμήματος πληροφορικής και το σημαντικότερο η εκπαίδευση όλου του προσωπικού σχετικά με τον κανονισμό.

7.1 Προσωπικός προβληματισμός

Η σύνθεση του θεωρητικού πλαισίου έχει αναλυθεί στη διατριβή. Για να κατανοήσουμε το ερευνητικό φαινόμενο, πολλά ερευνητικά άρθρα, σημαντικά έργα και βασικές έρευνες έχουν μελετηθεί και δοκιμαστεί συστηματικά. Οι επιλεγμένες θεωρίες σχετίζονται με τον Γενικό Κανονισμό Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR – General Data Protection Regulation) στο χώρο της υγείας και τον σχεδιασμό και την εφαρμογή των απαραίτητων τεχνολογιών πληροφορικής σε έναν οργανισμό υγείας. Με τα ερωτηματολόγια και με τους σχετικούς συμμετέχοντες, ο ερευνητής απέκτησε μεγαλύτερη κατανόηση χρησιμοποιώντας ένα θεωρητικό πλαίσιο. Όλες οι πληροφορίες που διάβασε σχετικά με το θέμα είναι εξαιρετικές και συνεπείς με τη σημερινή διαχείριση του GDPR.

Αν και οι ερωτηθέντες σχετίζονται με το θέμα της διατριβής, αντιπροσωπεύουν διαφορετικούς τομείς του θέματος. Η επικοινωνία με τους ερωτηθέντες παρείχε κάποιες πληροφορίες που δύσκολα θα βρίσκονταν απλώς κοιτάζοντας τα σχετικά επιστημονικά άρθρα και τη βιβλιογραφία καθώς προέρχονταν από άμεση εμπειρία. Οι πιο απαιτητικές και χρονοβόρες στιγμές ήταν η εύρεση παραδειγμάτων GDPR σε νοσοκομεία ή/και κλινικές στο εξωτερικό και η ανάλυση των ερωτηματολογίων και η συσχέτιση μεταξύ τους. Η πρόκληση ήταν να επιλεχθούν ποια δεδομένα θα χρησιμοποιηθούν και να συνδυαστούν με τρόπο τόσο αμερόληπτο όσο και ενδιαφέρον.

Ο ερευνητής πέρασε πολλές ώρες κάνοντας αυτό το έργο, αλλά μέσω αυτού έμαθε ότι αν δεν θέσει τους στόχους, δεν μπορεί να κάνει τίποτα. Δεν ήταν πάντα ο εαυτός του, αλλά, σε αυτήν την περίπτωση, του άρεσε η πρόκληση και ένιωσε ότι έκανε ότι μπορούσε. Έμαθε ότι όταν του αρέσει αυτό που κάνει, είναι πολύ πιο εύκολο για εκείνον να ξεχωρίσει. Επιπλέον, εργαζόμενος υπό την επίβλεψη του καθηγητή του, του έδωσε την ευκαιρία να αναπτύξει μια σχέση μέντορα / μαθητή με έναν επαγγελματία του κλάδου. Συνολικά, ήταν μια πολύτιμη και ευχάριστη εμπειρία.

7.2 Προτάσεις για περαιτέρω έρευνα

Σε σημασία με τους περιορισμούς της έρευνας, οι συστάσεις για επιπλέον έρευνα περιλαμβάνουν τα ακόλουθα σημεία:

- Δεδομένου ότι το δείγμα της μελέτης ήταν περιορισμένο, οι μελλοντικές μελέτες μπορούν να πραγματοποιήσουν μεγαλύτερο φάσμα συμμετεχόντων με περισσότερους οργανισμούς να λαμβάνουν μέρος.
- Η διατριβή βασίστηκε σε δύο πόλεις της Κύπρου. Μελλοντικά έργα μπορούν να διερευνήσουν το ρόλο του GDPR στο χώρο της υγείας στις άλλες πόλεις της Κύπρου.
- Άλλες εργασίες χρησιμοποιούν επίσης ποιοτικές ερευνητικές προσεγγίσεις που θα επιτρέψουν την εκτίμηση των εξεταζόμενων θεμάτων.

Βιβλιογραφία

- Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H. And Saadi, M., 2017. Big data security and privacy in healthcare: A Review. Procedia Computer Science, **113**, pp. 73 - 80.
- Al Omar, A., Rahman, S.M., Basu, A. And Kiyomoto, S., 2017. MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data, The 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage 2017, ResearchGate.
- Austin, C. And Kusumoto, F., 2016. The application of Big Data in medicine: current implications and future directions. Journal of Interventional Cardiac Electrophysiology, **47**, pp. 51 - 59.
- Australian entities and the EU General Data Protection Regulation (GDPR). 2018. Australian: Office of the Australian Information Commissioner.
  Available: https://dhadjinestoros.com/portfolio-galleries/general-data-protection-regulation-gdpr-in-cyprus/ [September 21, 2020].
- Behlow J-D. And Aumage, V., June 2016, 2016-last update, Health data and data privacy: challenges for data processors under the GDPR [Homepage of Taylor Wessing Global Data Hub], [Online]. Available: https://globaldatahub.taylorwessing.com/article/health-data-and-data-privacy-challenges-for-data-processors-under-the-gdpr [September 20, 2020].
- Chahal, S., 2019. GDPR And Accessing Medical Records - A Practice Manager's Guide. https://www.firstpracticemanagement.co.uk/blog/gdpr-and-accessing-medical-records-a-practice-managers-guide/: First Practice Management.
- Chilvers, A., 2018. GDPR and what it means for healthcare providers. https://www.bjfm.co.uk/gdpr-and-what-it-means-for-healthcare-providers#:~:text=From%20May%2025%2C%202018%2C%20the,store%20all%20their%20personal%20information.&text=Keeping%20confidential%20information%20about%20staff,have%20taken%20seriously%20for%20years. edn. British Journal of Family Medicine.
- Christy, R. and Rochon, N., 2018. How will the GDPR affect the processing of employee health information? https://www.personneltoday.com/hr/gdpr-employee-health-information/: Personnel Today.
- Chubb, 2019. Five consequences of a GDPR breach. The Telegraph. ISSN https://www.telegraph.co.uk/business/risk-management-solutions/consequences-of-gdpr-breach/#:~:text=Companies%20that%20fail%20to%20comply,negligence%20and%2For%20wrongful%20acts.
- Corporate Information Governance, 2019. NHS England and NHS Improvement - Confidentiality Policy. v5.1. England.
- Creswell, J. (2003). Research design: Qualitative, quantitative and mixed methods approaches (2nd ed.). Thousand Oaks, CA: SAGE Publications.

- Dimitrov, V.D., 2019. Blockchain Applications for Healthcare Data Management. https://synapse.koreamed.org/articles/1115984?fbclid=IwAR2FWJfAQj4ATD0XSJ4rhISI8KsgPcZ7qxy0nh7DGDxnELjNWQ811FO93uE edn. Bulgaria: Health Inform Res.
- European Commission, What are the responsibilities of a Data Protection Officer (DPO). Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo_en?fbclid=IwAR2-gDwpTqdgGxlP03VVUleCUVElQz5EXurDtVaLX8EvZPq5OGyRE5HqKu8 [October 25, 2020].
- Fernández-Alemán, J.L., Carrión Señor, I., Lozoya, A.O.P. And Toval, A., 2013. Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46, pp. 541 - 562.
- GDPR challenges for the health care sector. 2019.
- GDPR Enforcement and Fines Have Arrived. 2020. Beazley Breach Insights.
- GDPR Fines. https://easygdpr.eu/gdpr-fines/: easyGDPR governance platform.
- GDPR, 2018. Healthcare sector: How to Comply With GDPR?
- GDPR: are you unknowingly breaching the law? 2019.
- General Data Protection Regulation (GDPR) in Cyprus [Homepage of Hadjinestoros LLC], [Online].
- Grafimedia Gr, 2020-last update, Κανονισμός GDPR. Available: https://grafimedia.eu/gr/efarmogi-kanonismou-gdpr/ [October 31, 2020].
- Guide to GDPR Compliance for US Companies. 2020. Reciprocity.
- Health data in the workplace [Homepage of European Data Protection Supervisor], [Online]. Available: https://edps.europa.eu/data-protection/data-protection/reference-library/health-data-workplace_en [September 23, 2020].
- https://www.appoint.co.uk/2019/02/11/gdpr-breaching-law/: Appoint Recruitment. https://www.gdprregister.eu/gdpr/healthcare-sector-gdpr/: GDPR register. https://www.tgsbaltic.com/en/publications/gdpr-challenges-for-the-health-care-sector/: TGS Baltic.
- Ioannidou, V., 2019. European Union: The GDPR and the Effect On The Medical Profession. https://www.mondaq.com/cyprus/data-protection/861664/the-gdpr-and-the-effect-on-the-medical-profession: mondaq - Connecting knowledge & people.
- Kades, A., 2020. Cyprus has dealt with 740 GDPR complaints since regulation enforced. CyprusMail. ISSN https://cyprus-mail.com/2020/05/25/cyprus-has-dealt-with-740-gdpr-complaints-since-regulation-enforced/.
- Katuwal, J.G., Pandey, S., Hennessey, M. And Lamichhane, B., 2018. Applications of Blockchain in Healthcare: Current Landscape & Challenges. A Preprint.
- Kefron, Data Protection in Hospitals: How to Rectify GDPR Failings in The Hospital Sector. Kefron - The information Management People.
- Ledger Insights, 2020. Cyprus hospital adopts blockchain medical data solution from VeChain. https://www.ledgerinsights.com/cyprus-hospital-blockchain-medical-data-vechain/: Ledger Insights.
- Leedy, P. & Ormrod, J. (2001). Practical research: Planning and design (7th ed.). Upper Saddle River, NJ: Merrill Prentice Hall. Thousand Oaks: SAGE Publications.

- Li, H., Yu, L. And He, W., 2019. The Impact of GDPR on Global Technology Development. Journal of Global Information Technology Management, **22**(1), pp. 1 - 6.
- Lopes, M.I. And Oliveira, P., 2018. Evaluation of the Implementation of the General Data Protection Regulation in Health Clinics. Journal of Information Systems Engineering & Management, **3**(4).
- Marciniak, E., 2019. Protection of Health Data in Accordance With The GDPR: Selected Issues. Journal of the European Union, **16**(2), pp. 87 - 100.
- Markopoulou, V., Nieri, A., Liaskos, J., Zoulias, E. and Mantas, J., 2020. Nursing Staff's Awareness of Processing Personal Data According to GDPR. The Importance of Health Informatics in Public Health during a Pandemic.
- Martínez, S., Sánchez, D. And Valls, A., 2013. A semantic framework to protect the privacy of electronic health records with non-numerical attributes. Journal of Biomedical Informatics, **46**, pp. 294 - 303.
- Media, 2018. GDPR: 7 keys to comply with the GDPR in hospitals and clinics. https://blog.signaturit.com/en/gdpr-7-key-points-for-hospitals-and-clinics: Signaturit.
- Miliard, M., 2018. European perspective: How hospitals should be approaching GDPR compliance. https://www.healthcareitnews.com/news/emea/european-perspective-how-hospitals-should-be-approaching-gdpr-compliance#:~:text=GDPR%20has%20a%20higher%20compliance,U.S.%20hospitals%20think%20of%20it.: Healthcare IT News.
- Moore, D. and McCabe, G. (2005) Introduction to the practice of statistics. 5th edn. W.H. Freeman & Company Publications.
- Patients and Privacy: GDPR Compliance for Healthcare Organizations. 2018. https://www.trendmicro.com/vinfo/dk/security/news/online-privacy/patients-and-privacy-gdpr-compliance-for-healthcare-organizations: Trend Micro.
- Regulation (Eu) 2016/679 of the European Parliament and of the Council. 2016. Official Journal of the European Union.
- RohatgI, J., 2018. GDPR and healthcare: Understanding health data and consent. https://www.pega.com/insights/articles/gdpr-and-healthcare-understanding-health-data-and-consent: PEGA.
- Sousa, M., Ferreira, D., Santos-Pereira, C., Bacelar, G., Frade, S., Pestana, O. And Cruz-Correia, R., 2018. OpenEHR Based Systems and the General Data Protection Regulation (GDPR). Building Continents of Knowledge in Oceans of Data: The Future of Co-Created eHealth.
- Stockwell, E. And Hill, D., 2018. GDPR frequently asked questions for healthcare professionals. Hill Dickinson.
- Sturman, C., 2020. GDPR - Is healthcare ready? https://www.healthcareglobal.com/digital-healthcare/gdpr-healthcare-ready: Healthcare.
- The Data Protection Bill - New Criminal Offences for Data Protection Breaches On Their Way to the Statute Book. 2018. https://www.kingsleynapley.co.uk/insights/blogs/data-protection-blog/the-data-protection-bill-new-criminal-offences-for-data-protection-breaches-on-their-way-to-the-statute-book: Kingsley Napley.

- Vashkover, A., 2019. After the Dust Has Settled: GDPR in Healthcare. https://www.cybermdx.com/blog/after-the-dust-has-settled-gdpr-in-healthcare: Cyber MDX.
- Vasileiou Milona, D., 2013. Πληροφοριακά Συστήματα Υγείας, Πανεπιστήμιο Πειραιώς.
- Wallace, R. and Greene, E., 2019. Survey of NCHDs in Ireland to assess their views and opinions in relation to participation in health research and the impact of new Irish data protection regulations. Irish Journal of Medical Science.
- Whalen, A., 2017. Collecting and Handling Health Data in a GDPR World, wHealth week, 10 - 12 May 2017, HIMSS Europe Gmbh, pp. 1 - 18.
- What Countries are Covered by GDPR? August 6, 2019, 2019-last update [Homepage of Reciprocity], [Online]. Available: https://reciprocitylabs.com/resources/what-countries-are-covered-by-gdpr/ [September 23, 2020].
- Why and how GDPR applies to companies globally. https://privacyinternational.org/long-read/2207/why-and-how-gdpr-applies-companies-globally#:~:text=The%20GDPR%20is%20extraterritorial%20in,any%20company%20in%20the%20world.&text=However%2C%20if%20those%20companies%20also,need%20to%20comply%20with%20GDPR.: Privacy International.
- Williams, C., 2007. Research Methods. *Journal of Business & Economic Research,* **5**(3)
- Yuan, B. And Li, J., 2019. The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. International Journal of Environmental Research and Public Health, **16**(1070), pp. 1 - 15.
- Κουτσούκογλου, Α., 2019. Προσωπικά δεδομένα στον χώρο της υγείας και ηλεκτρονικές εφαρμογές υγείας, Πανεπιστήμιο Μακεδονίας Δημοκρίτειο Πανεπιστήμιο Θράκης.
- Πλατής, Ε., 2018. Προσωπικά Δεδομένα Προστασία GDPR. Αθήνα: Κυριάκος Παπαδόπουλος Α.Ε.
- Συμμόρφωση με τον GDPR, 2020-last update, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων και η GDPR Experts Team. Available: https://www.bmlsecurity.gr/yphresies/%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%AF%CE%B5%CF%82-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD/%CF%83%CF%85%CE%BC%CE%BC%CF%8C%CF%81%CF%86%CF%89%CF%83%CE%B7-%CE%BC%CE%B5-%CF%84%CE%BF%CE%BD-gdpr [October 31, 2020].

Παραρτήματα

9.1 Ερωτηματολόγιο

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR) ΣΤΗΝ ΥΓΕΙΑ ΚΑΙ Η ΕΦΑΡΜΟΓΗ ΤΟΥ ΣΤΗΝ ΚΥΠΡΟ

Σκοπός του ερωτηματολογίου είναι η συλλογή πληροφοριών σχετικά με τον νέο κανονισμό και την εφαρμογή του στον τομέα της υγείας στην Κύπρο, η σύγκριση με άλλες χώρες και η ανάδειξη του επιπέδου της Κύπρου.
*Required

Σε ποια ηλικιακή ομάδα βρίσκεστε; *
- 20-30
- 30-40
- 40-50
- 50+

Χώρος Εργασίας; *
- Νοσοκομείο - Κλινική
- Ογκολογικό Κέντρο
- Κέντρο αποκατάστασης
- Ιατρείο (Ιδιωτικό ιατρείο, οδοντιατρείο, κ.τ.λ)

Θέση εργασίας; *
- Ιατρικό Προσωπικό
- Νοσηλευτικό Προσωπικό
- Άλλο παραϊατρικό Προσωπικό (Τεχνολόγοι, Φύσιο., Λογο., Εργοθερ., κ.τ.λ.)
- Γραμματειακό Προσωπικό
- Άλλο προσωπικό

Χειρίζεστε προσωπικά δεδομένα ασθενών ή προσωπικού της κλινικής σας? *
- Ναι
- Όχι

Σε περίπτωση που χρησιμοποιείτε ηλεκτρονικά αρχεία με προσωπικά δεδομένα, παρακαλώ επιλέξτε μια από τις παρακάτω απαντήσεις που εκφράζει καλύτερα την υφιστάμενη κατάσταση.
- Δεν χρησιμοποιώ κωδικούς, ανοίγοντας τον υπολογιστή βρίσκομαι στα αρχεία που χρειάζομαι

- Οι κωδικοί που χρησιμοποιώ είναι ατομικοί μου, δεν τους χρησιμοποιεί άλλος συνάδελφος και είναι ίδιοι εδώ και πολύ καιρό
- Οι κωδικοί που χρησιμοποιώ είναι ατομικοί μου, δεν τους χρησιμοποιεί άλλος συνάδελφος και αλλάζουν σε τακτά διαστήματα
- Οι κωδικοί που χρησιμοποιώ είναι κοινοί, τους χρησιμοποιούν και άλλοι συνάδελφοι και είναι ίδιοι εδώ και καιρό
- Οι κωδικοί που χρησιμοποιώ είναι κοινοί, τους χρησιμοποιούν και άλλοι συνάδελφοι και αλλάζουν σε τακτά διαστήματα

Γνωρίζετε για το νέο κανονισμό προστασίας προσωπικών δεδομένων που εφαρμόστηκε το 2018? *
- Ναι
- Όχι

Είχατε ενημέρωση για το νέο κανονισμό και τις αλλαγές που επιφέρει από τη διοίκηση του νοσοκομείου? *
- Ναι
- Όχι

Αν έγινε ενημέρωση με ποιόν τρόπο έγινε? *
- Επιστολή
- EMAIL
- Τμηματική ενημέρωση από τον υπεύθυνο τμήματος
- Σεμινάριο
- Δεν είχα ενημέρωση

Από την εφαρμογή του κανονισμού και έπειτα θεωρείτε ότι άλλαξε κάτι στο τρόπο που εργάζεστε? *
- Ναι
- Όχι

Αν η προηγούμενη απάντηση ήταν ναι, τότε σημειώστε τι ισχύει για έσας: *
- Αυξημένος Φόρτος Εργασίας
- Μειωμένη Παραγωγικότητα
- Καλύτερη προστασία των προσωπικών δεδομένων
- Καλύτερη Οργάνωση
- Κανένα από τα πιο πάνω

Από την εφαρμογή του κανονισμού και μέχρι σήμερα, άλλαξαν τα έντυπα ή/και κάποια ηλεκτρονικά αρχεία που χρησιμοποιούσατε; *
- Ναι
- Όχι

Πιστεύετε ότι στο νοσοκομείο που εργάζεστε εφαρμόζεται ικανοποιητικά ο κανονισμός προστασίας προσωπικών δεδομένων? *

ΚΑΘΟΛΟΥ
1
2
3
4
5
ΑΡΚΕΤΑ

Θεωρείτε ότι το νοσοκομείο που εργάζεστε μπορεί να βελτιωθεί όσον αφορά την εφαρμογή του κανονισμού προστασίας προσωπικών δεδομένων; *

- Ναι
- Όχι

Στο χώρο εργασίας σας υπάρχει εγχειρίδιο πολιτικών, διαδικασιών και εγγράφων για τη σωστή επεξεργασία προσωπικών δεδομένων; *

- Ναι
- Όχι

Πιστεύετε ότι χρειάζεστε περισσότερη ενημέρωση σχετικά με το κανονισμό προστασίας προσωπικών δεδομένων; *

- Ναι
- Όχι

Γνωρίζετε τα δικαιώματά σας που απορρέουν από τον Κανονισμό; *

- Ναι πλήρως
- Ναι μερικώς
- Όχι

Τι θα προτείνατε για καλύτερη εφαρμογή του κανονισμού στο νοσοκομείο που εργάζεστε;

Your answer

Εάν επιθυμείτε συμπληρώστε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας (email) για μελλοντικές έρευνες.

Your answer

Θεωρείτε το κανονισμό προστασίας προσωπικών δεδομένων σημαντικό στο τομέα τη Υγείας; *

ΚΑΘΟΛΟΥ

1
2
3
4
5

ΑΡΚΕΤΑ

9.2 Φύλλο Πληροφοριών Συμμετεχόντων

Φύση της έρευνας
Η φύση αυτής της μελέτης είναι να συνδεθούν οι κανονισμοί του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων στον τομέα της υγείας με την ανταπόκριση οργανωμένων ομάδων και υπεύθυνων φορέων στην Κύπρο με την εφαρμογή των νέων κανονισμών καθώς και να προσδιορίσει τον αντίκτυπο, τα πλεονεκτήματα και τις αδυναμίες των εκτελεστικών κανονισμών και προτείνετε πιθανές λύσεις και ενέργειες. Η έρευνα πραγματοποιείται από τον Αντρέα Χατζηπετρή, μεταπτυχιακό φοιτητή που σπουδάζει στην Σχολή θετικών και εφαρμοσμένων επιστημών, στο Ανοικτό Πανεπιστήμιο Κύπρου. Η έρευνα χρηματοδοτείται εξ ολοκλήρου από τον ερευνητή.
Τα δεδομένα συγκεντρώνονται σε ένα στάδιο με δομημένο ερωτηματολόγιο με πρόσωπα που εργάζονται σε διάφορα τμήματα σε οργανισμούς υγείας στην Κύπρο.

Επιπτώσεις της συμμετοχής και τα δικαιώματα όσων συμμετέχουν
Η συμμετοχή σε αυτή τη μελέτη είναι απολύτως εθελοντική. Οι συμμετέχοντες έχουν το δικαίωμα να αρνηθούν να απαντήσουν σε ερωτήσεις. Οι συμμετέχοντες έχουν τον έλεγχο του δικαιώματος καταγραφής και των απαντήσεων τους. Οι συμμετέχοντες μπορούν να αποχωρήσουν από τη μελέτη ανά πάσα στιγμή. Συμμετέχοντας σε αυτήν τη μελέτη, ανώνυμα σχόλια μπορούν να δημοσιευτούν σε ένδειξη. Ο ερευνητής εξασφαλίζει πλήρη εμπιστευτικότητα και ανωνυμία δεδομένων. Κανένας συμμετέχων δεν θα ονομάζεται μεμονωμένα εκτός από την αναφορά στον οργανισμό για να διασφαλιστεί η αξιοπιστία των πηγών.

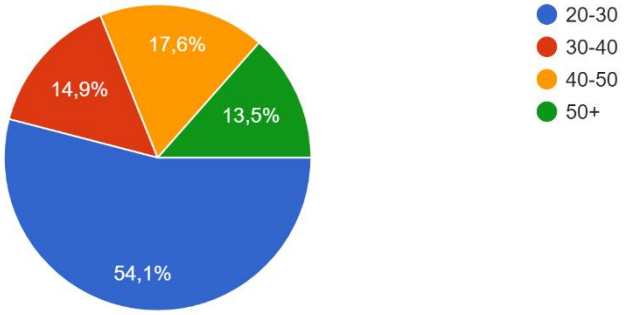
Χρήση δεδομένων και τρόπος με τον οποίο θα αναφέρονται
Ο ερευνητής είναι το μοναδικό άτομο που θα έχει πρόσβαση στα δεδομένα που συλλέγονται. Διαβεβαιώσεις σχετικά με την ανωνυμία και παραμένουν εμπιστευτικά μετά την ολοκλήρωση της έρευνας. Τα δεδομένα θα διατηρηθούν με ασφάλεια σε μια κρυπτογραφημένη εξωτερική συσκευή. Οι διασφαλίσεις για τη διασφάλιση του συνεχούς μέλλοντος εμπιστευτικά των δεδομένων και της ανωνυμίας των συμμετεχόντων θα λάβουν τη μορφή μιας εξωτερικής συσκευής που θα γνωρίζει μόνο ο ερευνητής που θα αντικαταστήσει όλες τις αναγνωρίσιμες ενδείξεις των συμμετεχόντων στην έρευνα.

Εάν έχετε οποιεσδήποτε ανησυχίες ή απορίες, μην διστάσετε να επικοινωνήσετε με τον ερευνητή.

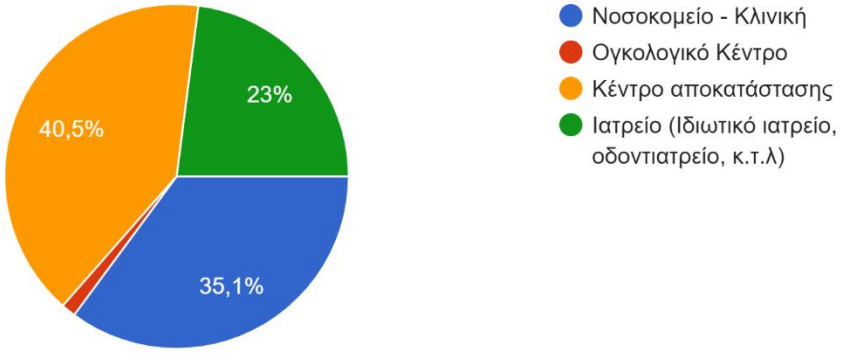
Ηλεκτρονικό ταχυδρομείο: antreas.hpetris@gmail.com **Κινητό**: (+357) 99043300

9.3 Πίνακες Αποτελεσμάτων

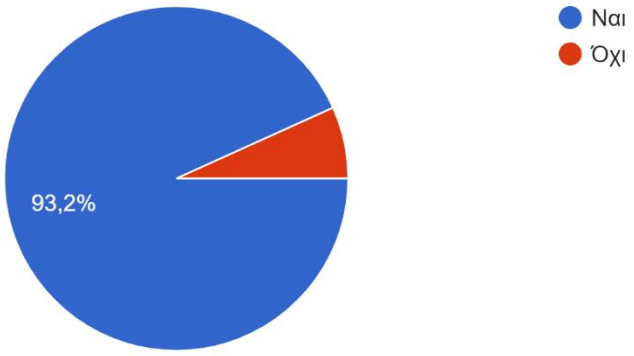
Σε ποια ηλικιακή ομάδα βρίσκεστε;
74 απαντήσεις



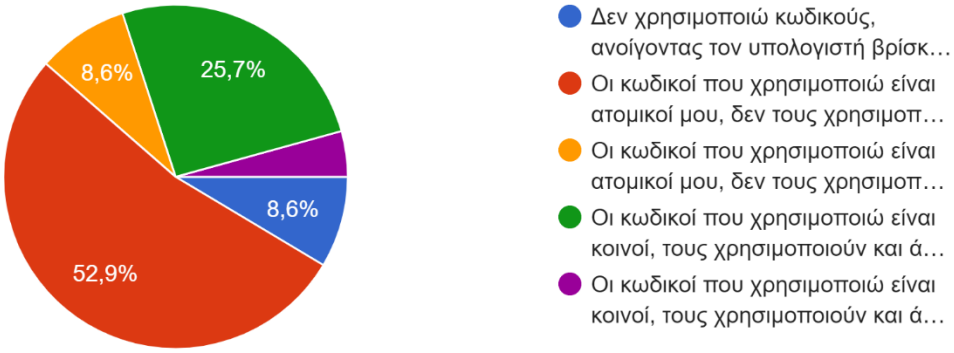
Χώρος Εργασίας;
74 απαντήσεις



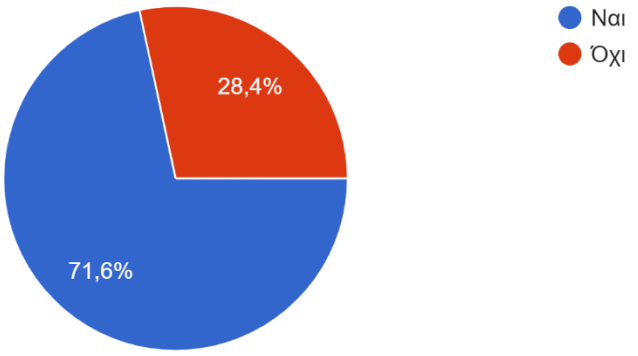
Χειρίζεστε προσωπικά δεδομένα ασθενών ή προσωπικού της κλινικής σας?
74 απαντήσεις



Σε περίπτωση που χρησιμοποιείτε ηλεκτρονικά αρχεία με προσωπικά δεδομένα, παρακαλώ επιλέξτε μια από τις παρακάτω α...ράζει καλύτερα την υφιστάμενη κατάσταση.
70 απαντήσεις

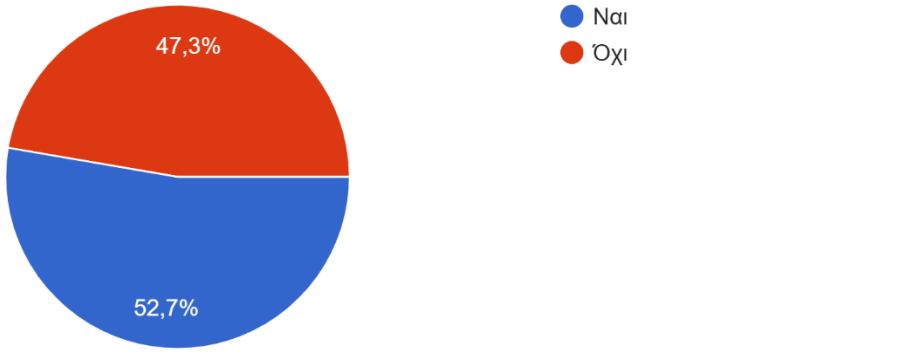


Γνωρίζετε για το νέο κανονισμό προστασίας προσωπικών δεδομένων που εφαρμόστηκε το 2018?
74 απαντήσεις



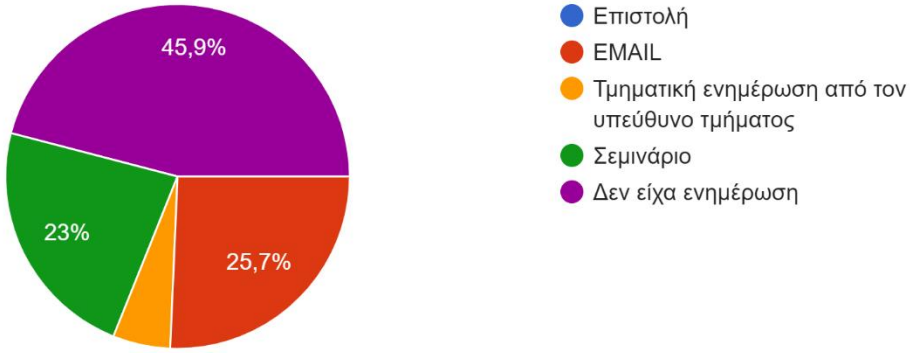
Είχατε ενημέρωση για το νέο κανονισμό και τις αλλαγές που επιφέρει από τη διοίκηση του νοσοκομείου?

74 απαντήσεις



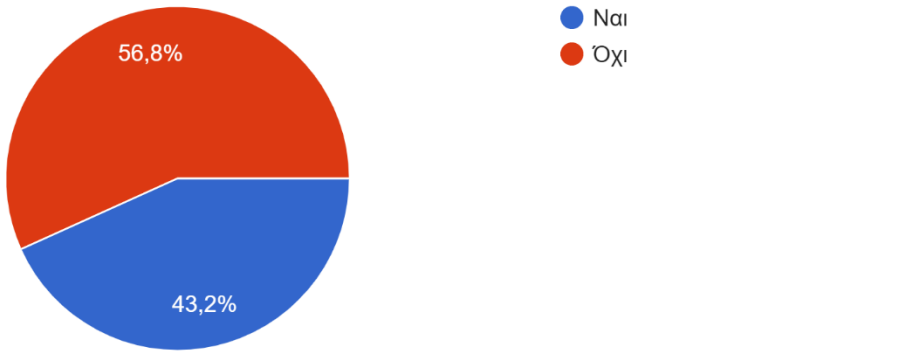
Αν έγινε ενημέρωση με ποιόν τρόπο έγινε?

74 απαντήσεις



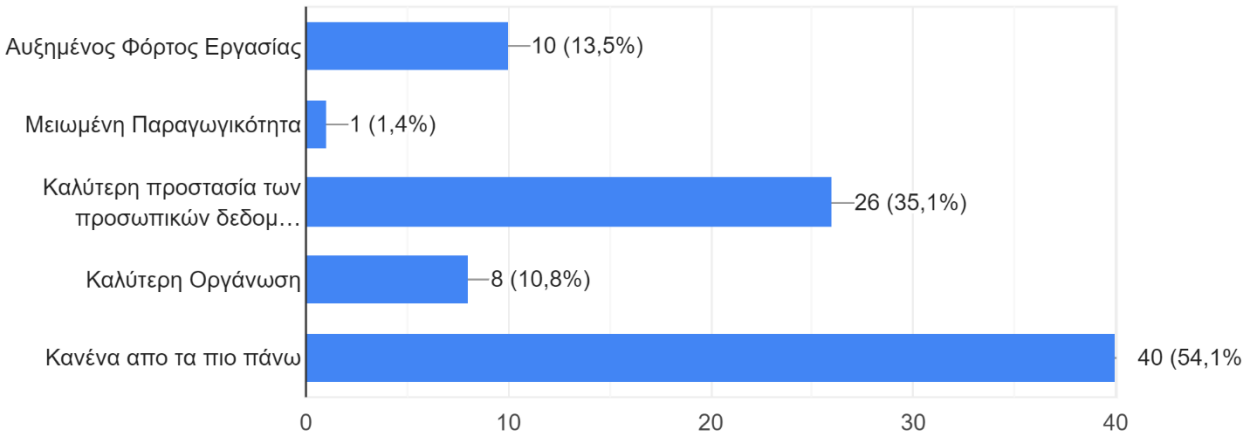
Από την εφαρμογή του κανονισμού και έπειτα θεωρείτε ότι άλλαξε κάτι στο τρόπο που εργάζεστε?

74 απαντήσεις



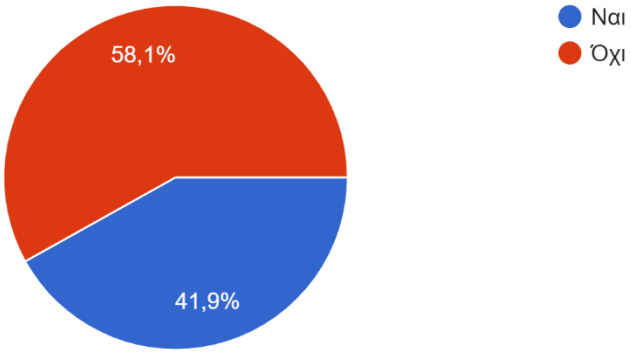
Αν η προηγούμενη απάντηση ήταν ναι, τότε σημειώστε τι ισχύει για έσας:

74 απαντήσεις



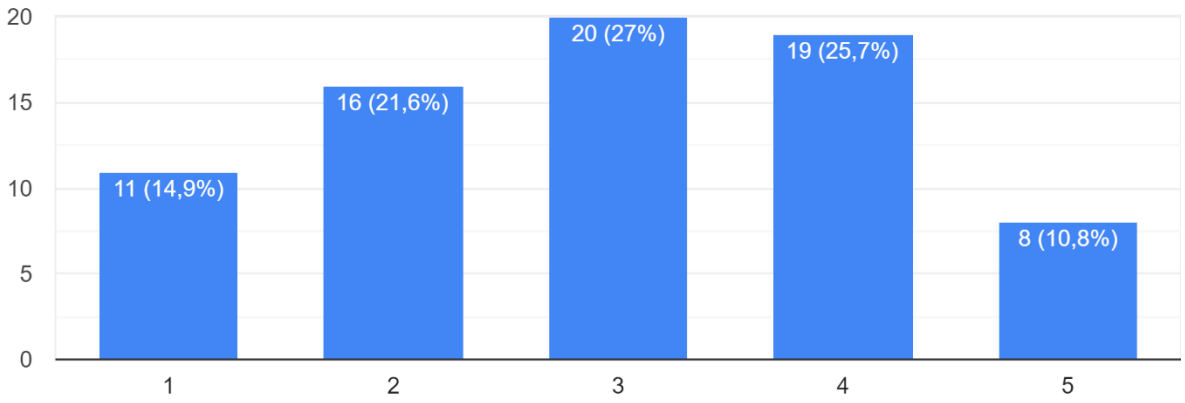
Από την εφαρμογή του κανονισμού και μέχρι σήμερα, άλλαξαν τα έντυπα ή/και κάποια ηλεκτρονικά αρχεία που χρησιμοποιούσατε;

74 απαντήσεις



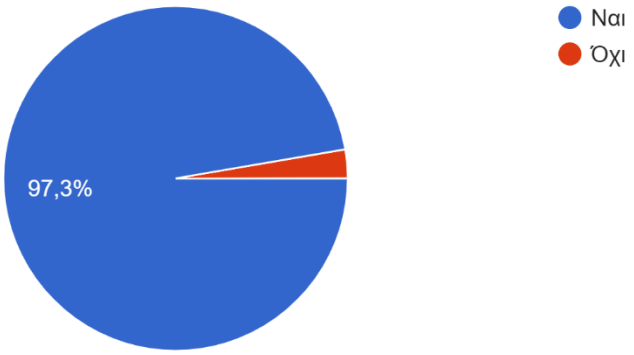
Πιστεύετε ότι στο νοσοκομείο που εργάζεστε εφαρμόζεται ικανοποιητικά ο κανονισμός προστασίας προσωπικών δεδομένων?

74 απαντήσεις



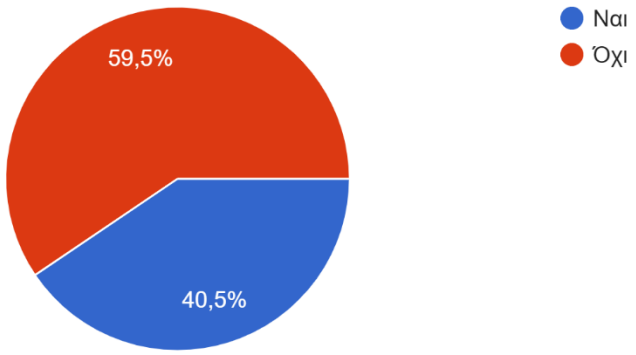
Θεωρείτε ότι το νοσοκομείο που εργάζεστε μπορεί να βελτιωθεί όσον αφορά την εφαρμογή του κανονισμού προστασίας προσωπικών δεδομένων;

74 απαντήσεις



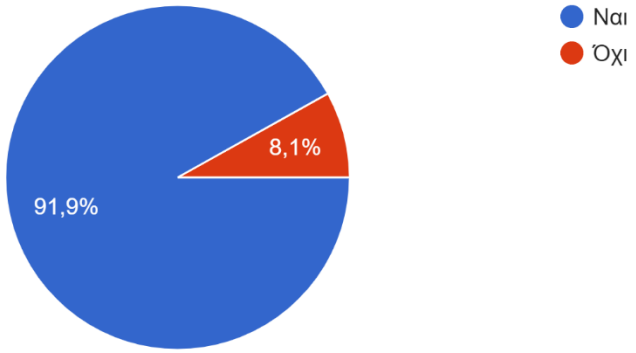
Στο χώρο εργασίας σας υπάρχει εγχειρίδιο πολιτικών, διαδικασιών και εγγράφων για τη σωστή επεξεργασία προσωπικών δεδομένων;

74 απαντήσεις



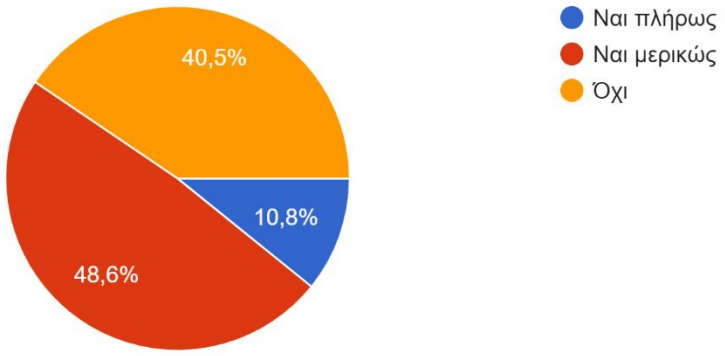
Πιστεύετε ότι χρειάζεστε περισσότερη ενημέρωση σχετικά με το κανονισμό προστασίας προσωπικών δεδομένων;

74 απαντήσεις



Γνωρίζετε τα δικαιώματά σας που απορρέουν από τον Κανονισμό;

74 απαντήσεις



Θεωρείτε το κανονισμό προστασίας προσωπικών δεδομένων σημαντικό στο τομέα τη Υγείας;

74 απαντήσεις