Θέμα διπλωματικής εργασίας: Εσωτερικός έλεγχος και προστασία προσωπικών δεδομένων στον κλάδο της υγείας. Τυπική συμμόρφωση ή προσθήκη αξίας;
Μελέτη Περίπτωσης: Σπηλιοπούλειο Νοσοκομείο «Η Αγία Ελένη».

Μεταπτυχιακή φοιτήτρια: ΚΟΝΤΕΑ ΦΑΙΔΡΑ

Α.Μ.: 00158

Εισηγητής: ΚΟΥΤΟΥΠΗΣ ΑΝΔΡΕΑΣ

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κύριο Κουτούπη Ανδρέα καθώς και όλη την ομάδα του για την πολύτιμη βοήθεια και καθοδήγησή τους.

Περιεχόμενα

1. Η έννοια και η σημασία του εσωτερικού ελέγχου

1.1 Ο ορισμός του εσωτερικού ελέγχου

Η διεθνοποίηση των εταιρειών, η αύξηση του ανταγωνισμού, οι τεχνολογικές καινοτομίες και οι πρόσφατες διεθνείς κρίσεις δημιούργησαν την ανάγκη βελτίωσης των διαδικασιών εταιρικής διακυβέρνησης, με τη διαχείριση κινδύνων να συμβάλλει θεμελιωδώς στην επίτευξη θεσμικών στόχων και του ορισμού της αποστολής των οργανισμών. Υπό αυτή την έννοια, αναπτύχθηκαν πρότυπα για τη διαχείριση κινδύνων και για τη λειτουργία των εσωτερικών ελέγχων σε οργανισμούς σε διάφορες χώρες, με την υιοθέτηση διεθνών προτύπων για εσωτερικούς ελέγχους, για την διακυβέρνηση και διαχείριση κινδύνων, όπως είναι για παράδειγμα τα πρότυπα της COSO, του «Διεθνούς Οργανισμού Τυποποίησης» (ISO), της «Ομοσπονδίας Ευρωπαϊκών Ενώσεων Διαχείρισης Κινδύνων» (FERMA) και της «Διεθνούς Ένωσης Επαγγελματικών Πρακτικών» (IPPF), με την τελευταία να προέρχεται από το Ινστιτούτο Εσωτερικών Ελεγκτών (IIA) (Chevers et al., 2016).

Με την υιοθέτηση των πρακτικών που χρησιμοποιούνται στον ιδιωτικό τομέα, η εταιρική διακυβέρνηση στον δημόσιο τομέα άρχισε να χρησιμοποιεί τη διαχείριση κινδύνων, σύμφωνα με το μοντέλο των τριών γραμμών, που υιοθετήθηκε από την IA (2013). Ιδιαίτερα στον τομέα της δημόσιας υγείας, οι ανησυχίες για τη χρηματοοικονομική και λειτουργική βιωσιμότητα, που προκαλούνται από οικονομικές κρίσεις που ενδέχεται να μειώσουν τις κρατικές χρηματοδοτικές συνεισφορές, καθώς και την εμφάνιση νέων πανδημιών που θα μπορούσαν να οδηγήσουν το σύστημα υγείας σε μια άνευ προηγουμένου κατάρρευση, καθιστούν απαραίτητη την υιοθέτηση στρατηγικών που μπορούν να προβλέψουν αυτούς τους κινδύνους ή να ελαχιστοποιήσουν τις επιπτώσεις τους, προκειμένου να διατηρηθεί η λειτουργία των φορέων υγείας.

Ως εκ τούτου, είναι απαραίτητο να υιοθετηθούν μηχανισμοί διακυβέρνησης, μεταξύ των οποίων είναι η διαχείριση κινδύνων και ο εσωτερικός έλεγχος έχει θεμελιώδη ρόλο στην αξιολόγηση της αποτελεσματικότητας αυτής της διαχείρισης. Επομένως, υπάρχει ανάγκη να γνωρίζουμε τον βαθμό στον οποίο έχει εφαρμοστεί η διαχείριση κινδύνου και ο ρόλος του εσωτερικού ελέγχου σε αυτή τη διαχείριση, σύμφωνα με την αντίληψη των ερωτηθέντων σε οργανισμούς δημόσιας υγείας.

Έτσι, διενεργήθηκε βιβλιογραφική ανασκόπηση, εμπειρικές ερευνητικές μελέτες, καθώς και ημιδομημένες συνεντεύξεις για την κατανόηση όχι μόνο της δομής διακυβέρνησης, αλλά και για να μάθουν οι ερευνητές τι συμβαίνει στην πρακτική αυτών των οργανισμών, σύμφωνα με την αντίληψη των ερωτηθέντων, οι οποίοι ασκούσαν, κατά το χρόνο των συνεντεύξεων, λειτουργίες εσωτερικού ελέγχου στους αναλυθέντες οργανισμούς υγείας.

Ο κίνδυνος είναι μέρος των δραστηριοτήτων των οργανισμών, αφού οποιαδήποτε ενέργεια εμπεριέχει έναν ορισμένο βαθμό κινδύνου. Ο κίνδυνος μπορεί να οριστεί ως η «επίδραση της αβεβαιότητας στους στόχους» για το ISO 31000 (2018). Αυτή η επίδραση είναι μια απόκλιση από αυτό που θα αναμενόταν και μπορεί να είναι θετική (ευκαιρία) ή αρνητική (κίνδυνος). Σύμφωνα με την COSO (2007), «η αρχή που ενυπάρχει στη διαχείριση εταιρικού κινδύνου είναι ότι κάθε οργανισμός υπάρχει για να παράγει αξία για τα ενδιαφερόμενα μέρη».

Η αντιμετώπιση των κινδύνων πρέπει να οδηγεί σε υπολειπόμενους κινδύνους σύμφωνα με την διάθεση για κινδύνους, προκειμένου να διασφαλιστεί η επίτευξη των στόχων της οντότητας (Ribeiro, 2020). Είναι σημαντικό να διευκρινιστεί ότι η διαχείριση κινδύνων, από μόνη της, δεν προσφέρει απόλυτη εγγύηση για την οικονομική οντότητα, ειδικά όσον αφορά πιθανές ζημίες και συμπαιγνία. (COSO, 2007).

Σύμφωνα με την COSO (2007), ο εσωτερικός ελεγκτής έχει το ρόλο της αξιολόγησης της διαχείρισης κινδύνου σε συνεχή βάση, προκειμένου να βελτιώσει την αποτελεσματικότητα της διαδικασίας και την οργανωτική απόδοση, εκτός από τη δημιουργία χρήσιμων πληροφοριών για τα ανώτερα στελέχη, για την υποστήριξη της λήψης αποφάσεων. υπέρ της εκπλήρωσης των θεσμικών στόχων.

Για το ISO 31000 (2018), η διαδικασία διαχείρισης κινδύνου «αποτελείται από τη συστηματική εφαρμογή πολιτικών, διαδικασιών και πρακτικών διαχείρισης που περιλαμβάνουν δραστηριότητες επικοινωνίας, διαβούλευσης, δημιουργίας του πλαισίου και αξιολόγησης, επεξεργασίας, παρακολούθησης, καταχώρισης και αναφοράς των κινδύνων».

Για τον Ferma, η διαχείριση κινδύνου είναι η διαδικασία μέσω της οποίας οι οργανισμοί αναλύουν μεθοδικά τους κινδύνους που ενυπάρχουν στις αντίστοιχες δραστηριότητές τους, με στόχο την επίτευξη ενός σταθερού πλεονεκτήματος σε κάθε μεμονωμένη δραστηριότητα και στο σύνολο όλων των δραστηριοτήτων (Ferma, 2003).

Επίσης, σύμφωνα με την COSO (2009), η διαχείριση κινδύνου δεν πρέπει να περιορίζεται σε μια συγκεκριμένη ομάδα ή τομέα, θα πρέπει να εφαρμόζεται στον οργανισμό ως σύνολο, και αυτό συνεπάγεται τη δημιουργία μιας κουλτούρας κινδύνου για όλους τους εργαζόμενους. Αυτή η κουλτούρα θα πρέπει να οδηγήσει στην ανάπτυξη αξιών και στάσεων, προκειμένου να προαχθεί η ακεραιότητα και να εντοπιστούν όλα τα γεγονότα που μπορεί να έχουν αντίκτυπο στην επίτευξη των οργανωτικών στόχων.

Εξάλλου, η επιστημονική έρευνα των οικονομικών καταστάσεων που σχετίζονται με τον έλεγχο, όπως οι συμβάσεις ελέγχου, τα οικονομικά κίνητρα και οι διαδικασίες ελέγχου, είναι σχετικά νέα. Μέχρι τη δεκαετία του 1970, ο έλεγχος θεωρούνταν μια πρακτική δραστηριότητα που διέπεται από τις διαδικασίες και τους τεχνικούς κανόνες που σχετίζονταν ευρύτερα με το επάγγελμα. Ωστόσο, ο έλεγχος είναι μια επαγγελματική δραστηριότητα που ασκείται στην ευρεία οικονομία μέσω κανόνων εφαρμογής και παρακολούθησης στις χρηματοοικονομικές λειτουργίες των οργανισμών και των επιχειρήσεων (Simunic & Wu, 2009).

Ο έλεγχος αναγνωρίστηκε ως επάγγελμα στα τέλη της δεκαετίας του εβδομήντα του περασμένου αιώνα. Αυτό το γεγονός οδήγησε σε αύξηση του ενδιαφέροντος για αυτό, ως ουσιαστικό μέρος της ανώτερης διοίκησης σε οργανισμούς, καθώς παρέχει υπηρεσίες σε ανώτερα διοικητικά συμβούλια μέσω επιτροπών ελέγχου (Brink & Witt, 1982). Ο έλεγχος χρηματοοικονομικών λειτουργιών είναι μια σημαντική εργασία για πολλά μέρη, όπως για τους μετόχους,

τους τρέχοντες και δυνητικούς πιστωτές και τους θεσμούς. Ο εσωτερικός έλεγχος (ΙΑ) ορίζεται σύμφωνα με το Ινστιτούτο Εσωτερικών Ελεγκτών ΙΙΑ (1999) ως μια αντικειμενική, ανεξάρτητη δραστηριότητα που παρέχει συμβουλευτικές υπηρεσίες για τη βελτίωση των λειτουργιών των οργανισμών για να τους προσθέσει αξία. Η ΙΑ δίνει τη δυνατότητα στους οργανισμούς να επιτύχουν τους στόχους τους ακολουθώντας το σύστημα, τους κανονισμούς και τις διαδικασίες για τη βελτίωση της διακυβέρνησης και του ελέγχου.

Οι οργανισμοί βασίζονται στην ΙΑ ως μία από τις κύριες λειτουργίες της συμβουλευτικής δραστηριότητας που προσθέτει αξία σε αυτά (Nagy & Cenker, 2002). Η λειτουργία ΙΑ ξεκίνησε με στόχο την καταπολέμηση της απάτης μέσω της επαλήθευσης των οικονομικών λειτουργιών των ιδρυμάτων. Οι λειτουργίες της ΙΑ στη διαχείριση και τον προγραμματισμό διαδραματίζουν θεμελιώδη και σημαντικό ρόλο στην προώθηση και τη βελτίωση της χρηστής διακυβέρνησης (Christopher, 2019). Η ΙΑ είναι ένας από τους μηχανισμούς εσωτερικού ελέγχου για τη βελτίωση και την ενίσχυση της διακυβέρνησης.

Τα τελευταία χρόνια, το έργο των ελεγκτών έχει επεκταθεί από την παραδοσιακή εργασία της ανίχνευσης απάτης στην εκτέλεση πολλών εργασιών όπως (Deloitte, 2018):

(i) η εργασία στην εκτίμηση του ηλεκτρονικού κινδύνου,

(ii) η διερεύνηση της οργανωσιακής κουλτούρας,

(iii) η αξιολόγηση της γενικής απόδοσης και

(iv) διασφάλιση της εφαρμογής γενικών κανονισμών και διαδικασιών για την προστασία των οικονομικών δεδομένων μέσω της χρήσης πολλών σύγχρονων προσεγγίσεων όπως η ανάλυση της δυναμικής και οπτικής απεικόνισης των αναφορών εκτός από την ανάλυση ευέλικτων πρακτικών

Σύμφωνα με αυτές τις διαδικασίες και τις ενημερώσεις που έχουν συμβεί, η χρήση της ΙΑ έχει γίνει ευρέως διαδεδομένη ως ένας από τους πιο εξέχοντες μηχανισμούς που χρησιμοποιούνται για τον έλεγχο των οικονομικών καταστάσεων. Παρά αυτή τη σημαντική και ουσιαστική εξέλιξη στις λειτουργίες ελέγχου, ο έλεγχος

αντιμετωπίζει σημαντική κριτική λόγω αδυναμίας εκτέλεσης της λειτουργίας όπως ορίζεται από τη ΙΙΑ. Η αποτυχία της εταιρείας Enron ήταν ένας από τους κύριους λόγους για τους οποίους επικρίθηκε η ΙΑ αφού φάνηκε η αδυναμία της να πετύχει τους βασικούς της στόχους όπως απαιτείται. Ωστόσο, σε γενικές γραμμές, οι λειτουργίες ΙΑ προσθέτουν αξία στους οργανισμούς και τις επιχειρήσεις, αν και η πρακτική πραγματικότητα είναι διαφορετική από αυτό που αναμένεται να γίνει σύμφωνα με τα διεθνή πρότυπα. Μπορεί να προταθεί ότι υπάρχει ένα κενό γύρω από τον ρόλο της ΙΑ στην εκτέλεση των καθηκόντων της για την επίτευξη προστιθέμενης αξίας στους οργανισμούς.

Σύμφωνα με τα αποτελέσματα του Christopher (2019), το κενό απόδοσης στις λειτουργίες ΙΑ προκύπτει λόγω έλλειψης σαφήνειας οπτικής όσον αφορά την οργανωτική θέση της ΙΑ (όπως ένα μέλος του διοικητικού συμβουλίου έναντι ενός εταίρου διαχείρισης), την λειτουργία της ΙΑ όπως για παράδειγμα η διαβεβαίωση έναντι της συμβουλευτικής, οι οικονομικές ή λογιστικές δεξιότητες και εμπειρίες των εσωτερικών ελεγκτών και ο βαθμός συμμετοχής τους στη ΙΙΑ και ο βαθμός στον οποίο οι εσωτερικοί ελεγκτές συμμορφώνονται με τα πρότυπα που διέπουν το επάγγελμα της ΙΑ κατά την άσκηση των καθηκόντων τους. Έτσι, οι αδύναμες λειτουργικές ρυθμίσεις και τα χαρακτηριστικά των εσωτερικών ελεγκτών είναι από τους κύριους λόγους για τον αναποτελεσματικό εσωτερικό έλεγχο.

1.2. Εσωτερικός έλεγχος και σύστημα εσωτερικού ελέγχου

Ο εσωτερικός έλεγχος, σύμφωνα με το ΙΙΑ, σχεδιάζεται και εκτελείται έτσι ώστε η διαχείριση να σχεδιάζει, να οργανώνει και να κατευθύνει την εκτέλεση επαρκών ενεργειών για να διασφαλίσει ότι οι στόχοι θα επιτευχθούν. Εξάλλου, ο εσωτερικός έλεγχος προϋποθέτει την ύπαρξη σχεδίου και συντονισμένων συστημάτων ελέγχων που σχετίζονται με τον έλεγχο, ως αποτέλεσμα της ευαισθησίας τέτοιων ελέγχων για την πρόληψη, τον εντοπισμό και την ουσιαστική διόρθωση σχετικών ελλείψεων ή στρεβλώσεων.

Σύμφωνα με το TCU (2009) οι εσωτερικοί έλεγχοι και τα συστήματα εσωτερικού ελέγχου είναι συνώνυμες εκφράσεις, που χρησιμοποιούνται για να αναφέρονται στη διαδικασία που αποτελείται από τους κανόνες της οργανωτικής δομής και το σύνολο των πολιτικών και διαδικασιών που υιοθετεί ένας οργανισμός για επιτήρηση, επιθεώρηση και επαλήθευση, η οποία επιτρέπει την πρόβλεψη , την παρατήρηση, τη διεύθυνση ή τη διοίκηση γεγονότων που μπορεί να επηρεάσουν την επίτευξη των στόχων του. (TCU, 2009).

Σύμφωνα με την TCU (2009), το σύστημα εσωτερικού ελέγχου είναι ευθύνη της διοίκησης της οντότητας και αποτελεί μια ολοκληρωμένη διαδικασία, που καλύπτει όλα τα επίπεδα, τις δραστηριότητες και τα καθήκοντα του οργανισμού, που χρησιμοποιείται ως μέσο για την επίτευξη των οργανωτικών στόχων και την αντιμετώπιση των κινδύνων.

Για το Αμερικανικό Ινστιτούτο Ορκωτών Λογιστών – AICPA, ένα αποτελεσματικό σύστημα εσωτερικού ελέγχου, από μόνο του, δεν μπορεί να δώσει απόλυτη εγγύηση ότι ο οργανισμός θα είναι επιτυχής, καθώς όλα τα συστήματα έχουν εγγενείς περιορισμούς, με πιθανότητα εμφάνισης δυσλειτουργιών, σφαλμάτων ή λαθών (AICPA, 2005).

Έτσι, συνιστάται η ύπαρξη υπηρεσίας με τη λειτουργία επαλήθευσης της αποτελεσματικότητας του Συστήματος Εσωτερικού Ελέγχου – SCI, και αυτός ο ρόλος έχει ασκηθεί από τον εσωτερικό έλεγχο, ο οποίος έχει εξελιχθεί από έναν απλό έλεγχο νομικής και λογιστικής συμμόρφωσης σε μια συνάρτηση αξιολόγησης της αποτελεσματικότητας της SCI με βάση τους κινδύνους, επιπλέον του ρόλου της παροχής συμβουλών (Ribeiro, 2020).

Σύμφωνα με τον Fulop (2017), η εργασία των ελεγκτών είναι απαραίτητη στις διαδικασίες ελέγχου και διαχείρισης των οργανισμών και είναι απαραίτητο να εισαχθεί η κουλτούρα της διαχείρισης κινδύνου για τη βελτίωση της αποτελεσματικότητας των διαδικασιών εργασίας. Για τη Lima (2014), ο εσωτερικός έλεγχος «εμφανίζεται ως σημαντικός μοχλός υποστήριξης της διαχείρισης», καθώς δημιουργεί αξία και προσφέρει βεβαιότητα για τους εσωτερικούς ελέγχους της οντότητας.

Για τον Ferma (2003), ο ρόλος της λειτουργίας «διαχείρισης κινδύνου» μπορεί να κυμαίνεται από έναν μόνο υπεύθυνο έως ένα τμήμα μεγάλης κλίμακας. Η λειτουργία εσωτερικού ελέγχου θα είναι διαφορετική σε κάθε οργανισμό, καθώς θα μπορεί να γνωμοδοτεί για τους κινδύνους που δίνουν προτεραιότητα από τα διευθυντικά στελέχη μέσω ελέγχων και αξιολογήσεων διαχείρισης κινδύνων, καθώς και με παροχή συμβουλών για τους κινδύνους και τους εσωτερικούς ελέγχους που χρησιμοποιούνται για την αντιμετώπισή τους. Οι εσωτερικοί ελεγκτές μπορούν επίσης να παρέχουν πληροφορίες σχετικά με τους κινδύνους και τους εσωτερικούς ελέγχους στο διοικητικό συμβούλιο, την επιτροπή ελέγχου και άλλα όργανα διακυβέρνησης. Στο έργο του, ο εσωτερικός έλεγχος πρέπει να εγγυάται την ανεξαρτησία και την αντικειμενικότητά του.

1.3. Στόχοι εσωτερικού ελέγχου

Ο εσωτερικός έλεγχος είναι μια δυναμική και επαναληπτική διαδικασία που έχει σχεδιαστεί για να βοηθήσει τη διοίκηση να παραμείνει εστιασμένη στους λειτουργικούς και οικονομικούς στόχους του οργανισμού. Η εφαρμογή ενός συστήματος εσωτερικού ελέγχου παρέχει εύλογη βεβαιότητα σχετικά με την επίτευξη τριών στόχων: αποτελεσματικότητα και αποδοτικότητα των λειτουργιών, αξιοπιστία της αναφοράς και συμμόρφωση με τους ισχύοντες νόμους και κανονισμούς (COSO, 2013).

Οι επιχειρησιακοί στόχοι, οι οποίοι ποικίλλουν ανάλογα με τις επιλογές της διοίκησης, σχετίζονται με την επίτευξη της βασικής αποστολής μιας επιχείρησης και μπορεί να σχετίζονται με τη βελτίωση της ποιότητας και της καινοτομίας και τη μείωση του κόστους και του χρόνου παραγωγής. Οι στόχοι αναφοράς αφορούν την προετοιμασία αξιόπιστων αναφορών, συμπεριλαμβανομένων των οικονομικών ή μη χρηματοοικονομικών και εσωτερικών ή εξωτερικών εκθέσεων. Οι στόχοι συμμόρφωσης σχετίζονται με τη συμμόρφωση μιας επιχείρησης με νόμους και κανονισμούς κατά τη διάρκεια των επιχειρηματικών της δραστηριοτήτων. Οι τρεις στόχοι θα πρέπει να είναι αλληλεξαρτώμενοι, καθώς οι αντίστοιχες δραστηριότητες ελέγχου μπορεί να υποστηρίζουν ή να αλληλοεπικαλύπτονται (COSO, 2011).

Για παράδειγμα, ένας αποτελεσματικός εσωτερικός έλεγχος για την προστασία περιουσιακών στοιχείων από ζημιές (δηλαδή, ένας επιχειρησιακός στόχος) βοηθά στη διασφάλιση αξιόπιστης αναφοράς (δηλαδή ένας στόχος αναφοράς) όταν η διοίκηση βασίζεται αποκλειστικά σε διαρκή αρχεία αποθεμάτων χωρίς να διενεργεί περιοδική φυσική επιθεώρηση για τον εντοπισμό ζημιών αποθεμάτων.

Ενώ οι τρεις στόχοι εσωτερικού ελέγχου μπορεί να επηρεάζουν ο ένας τον άλλον και είναι σημαντικοί για την απόδοση ενός οργανισμού, μια ανασκόπηση της βιβλιογραφίας δείχνει ότι οι περισσότερες έρευνες για τον εσωτερικό έλεγχο έχουν επικεντρωθεί στο ICFR. Για παράδειγμα, πολυάριθμα έγγραφα που βασίζονται σε αρχεία εξετάζουν τους καθοριστικούς παράγοντες και τις συνέπειες της αποκάλυψης των ICD με έμφαση στις γνωστοποιήσεις που επιβάλλονται από το SOX 302 και το SOX 404.

Μελέτες που εξετάζουν τους καθοριστικούς παράγοντες των ICD διερευνούν αρκετά ποιοτικά χαρακτηριστικά της IAF σε συνδυασμό με τα χαρακτηριστικά της εταιρείας (π.χ. Lin et al., 2011). Ο προσδιορισμός των καθοριστικών παραγόντων είναι κρίσιμος, όπως υποδεικνύουν πολλές εμπειρικές μελέτες, με τις σημαντικές οικονομικές συνέπειες των ICDs. Οι ερευνητές προτείνουν ότι οι υλικές αδυναμίες στο ICFR επηρεάζουν αρνητικά τις αντιδράσεις της αγοράς στις ανακοινώσεις κερδών), το κόστος κεφαλαίου, την ποιότητα αναφοράς, την ακρίβεια των προβλέψεων των αναλυτών και τις καθυστερήσεις στην έκθεση ελέγχου (Munsif et al. ., 2012).

Όπως αναφέρθηκε προηγουμένως, λόγω περιορισμένων αρχειακών δεδομένων, σχετικά λίγοι ερευνητές έχουν ερευνήσει εμπειρικά τον εσωτερικό έλεγχο των λειτουργιών και της συμμόρφωσης. Αν και δεν εξετάζουν άμεσα τις λειτουργίες και τους στόχους συμμόρφωσης, οι ερευνητές γενικά προτείνουν μια θετική σχέση μεταξύ των επιτευγμάτων των τριών στόχων εσωτερικού ελέγχου.

Για παράδειγμα, οι Boritz & Lim (2008) προτείνουν μια θετική συσχέτιση μεταξύ του ICFR και της οικονομικής απόδοσης (δηλαδή, βελτιωμένη απόδοση από χαμηλότερο κόστος συμμόρφωσης με τους κανονισμούς και βελτιωμένες λειτουργίες). Οι Feng et al. (2015) υποστηρίζουν ότι, καθώς ορισμένοι έλεγχοι διαδραματίζουν τόσο λειτουργικούς ρόλους, όσο και ρόλους χρηματοοικονομικής

αναφοράς, θα πρέπει να υπάρχουν αμοιβαία ευεργετικά αποτελέσματα στην ποιότητα της χρηματοοικονομικής αναφοράς και στην απόδοση των επιχειρήσεων.

Εξετάζοντας τη συσχέτιση μεταξύ των αδυναμιών υλικού που σχετίζονται με το απόθεμα στο ICFR και της διαχείρισης αποθεμάτων των επιχειρήσεων, η μελέτη τους δείχνει μια θετική σχέση μεταξύ της ποιότητας του ICFR και των λειτουργιών της εταιρείας. Ομοίως, οι Cheng et al. (2017) παρέχουν συστηματικά στοιχεία για τη σχέση μεταξύ του αποτελεσματικού ICFR και της επιχειρησιακής αποτελεσματικότητας της εταιρείας.

Οι Kedia et al. (2016) βρίσκουν επίσης μια σημαντική συσχέτιση μεταξύ της κουλτούρας μη συμμόρφωσης μιας εταιρείας και του κινδύνου λανθασμένης αναφοράς οικονομικών στοιχείων. Επιπλέον, μια πρόσφατη μελέτη των Lawrence et al. (2017) παρέχει ενδείξεις ότι ο κίνδυνος λειτουργικού ελέγχου υποδηλώνει πιθανές αδυναμίες ελέγχου της χρηματοοικονομικής πληροφόρησης.

Συγκεκριμένα, οι Lawrence et al. (2017) μετρούν τον κίνδυνο λειτουργικού ελέγχου με δύο τρόπους: παραβιάσεις δεδομένων (δηλαδή επιθέσεις κυβερνοασφάλειας) και δείκτη κινδύνου ελέγχου που αναπτύχθηκε για αυτόν ακριβώς τον λόγο. Τα ευρήματά τους υποδεικνύουν ότι οι πληρεξούσιοι για τον κίνδυνο λειτουργικού ελέγχου σχετίζονται θετικά με επακόλουθες ελλείψεις οικονομικών αναφορών, επαναδιατυπώσεις, επιστολές σχολίων SEC και αμοιβές ελέγχου.

1.4. Ποιότητα λειτουργίας εσωτερικού ελέγχου

Μια αποτελεσματική IAF δημιουργεί προστιθέμενη αξία σε έναν οργανισμό βοηθώντας τη διοίκηση και το διοικητικό συμβούλιο να αξιολογήσουν και να βελτιώσουν την αποτελεσματικότητα της διαχείρισης κινδύνου, του εσωτερικού ελέγχου και των διαδικασιών εταιρικής διακυβέρνησης (Yee et al., 2008).

Αρκετές μελέτες, χρησιμοποιώντας διαφορετικούς μεσολαβητές, εξετάζουν τον τρόπο με τον οποίο τα χαρακτηριστικά ποιότητας της IAF επηρεάζουν τη

χρηματοοικονομική αναφορά ή την απόδοση εσωτερικού ελέγχου. Για παράδειγμα, οι Prawitt et al. (2009) κατασκεύασαν έναν συγκεντρωτικό δείκτη για το εταιρικό έτος8 για τη μέτρηση της ποιότητας του εσωτερικού ελέγχου και διαπίστωσαν ότι ο δείκτης ποιότητας σχετίζεται αρνητικά με τη διαχείριση κερδών.

Οι Lin et al. (2011) συμπληρώνουν τη μελέτη των Prawitt et al. εξετάζοντας τη σχέση μεταξύ της IAF και της ποιότητας της χρηματοοικονομικής αναφοράς μέσω της πρόληψης και του εντοπισμού ουσιωδών αδυναμιών. Συγκεκριμένα, οι Lin et al. (2011) διαπιστώνουν ότι τα χαρακτηριστικά της IAF (π.χ. επίπεδο εκπαίδευσης) και οι δραστηριότητες (δηλ. ενσωμάτωση τεχνικών διασφάλισης ποιότητας, ελεγκτικές δραστηριότητες που σχετίζονται με την οικονομική αναφορά και παρακολούθηση της αποκατάστασης) μπορούν να μειώσουν την πιθανότητα αποκάλυψης ουσιωδών αδυναμιών που αναφέρονται στην Ενότητα 404 του SOX.

Ο Ege (2015) παρέχει επίσης στοιχεία ότι η ποιότητα του εσωτερικού ελέγχου (δηλαδή η ικανότητα και η αντικειμενικότητα) σχετίζεται αρνητικά με την πιθανότητα κακής συμπεριφοράς της διοίκησης. Ομοίως, οι Abbott et al. (2016) υποδεικνύουν ότι η ποιότητα της IAF, όπως μετράται από την κοινή παρουσία ικανότητας και ανεξαρτησίας, επηρεάζει θετικά την ποιότητα της χρηματοοικονομικής πληροφόρησης.

1.5 Η σημασία του προγραμματισμού του εσωτερικού ελέγχου

Ο εσωτερικός έλεγχος θεωρείται η ραχοκοκαλιά ενός οργανισμού και θεωρείται ως το βασικό στοιχείο για την εφαρμογή του λογιστικού συστήματος. Ο προγραμματισμός εσωτερικού ελέγχου, από την άλλη πλευρά, είναι το πρώτο βήμα του εσωτερικού ελέγχου και είναι μια φάση κατά την οποία καθορίζονται ο σκοπός, το εύρος, η διάρκεια και οι πόροι του εσωτερικού ελέγχου που θα διεξαχθεί. Ο αποτελεσματικός σχεδιασμός εσωτερικού ελέγχου επιτρέπει στις δραστηριότητες ελέγχου να είναι ο καταλύτης για μια εταιρεία που προστατεύει και προσθέτει αξία στον οργανισμό (Matari et al., 2014).

Επιπλέον, ο αποτελεσματικός σχεδιασμός του εσωτερικού ελέγχου και η ιεράρχηση των προς έλεγχο μονάδων είναι σημαντικοί τόσο όσον αφορά την αποτελεσματική χρήση των εσωτερικών ελεγκτών όσο και την αποδοτική χρήση των οικονομικών πόρων. Για το λόγο αυτό, στους σημερινούς οργανισμούς με μεγάλη ποικιλία μονάδων, έχει καταστεί πολύ σημαντικό να προσδιορίζονται οι πιο επικίνδυνες συγκρίνοντας τα επίπεδα κινδύνου καθεμιάς και να κατευθύνουν τη δραστηριότητα εσωτερικού ελέγχου σε αυτές τις μονάδες, ώστε ο οργανισμός να κάνει την πιο αποτελεσματική χρήση του εσωτερικού λογιστικού έλεγχου.

Οι μέθοδοι λήψης αποφάσεων πολλαπλών κριτηρίων (Multi-criteria decision making, MCDM) χρησιμοποιούνται ευρέως για την κατάταξη των εναλλακτικών από διάφορους πιθανούς υποψηφίους που υπόκεινται σε ένα σύνολο κριτηρίων, και η ιεράρχηση των μονάδων για τη δραστηριότητα εσωτερικού ελέγχου μπορεί να θεωρηθεί ως ένα είδος προβλήματος MCDM (Kilic & Kaya, 2015).

Από την άλλη πλευρά, η αβεβαιότητα είναι χαρακτηριστικό του πραγματικού κόσμου και υπάρχει στη φύση των περισσότερων προβλημάτων MCDM. Τα κριτήρια σε αυτά τα προβλήματα είναι γενικά εκφρασμένα με ποιοτικό τρόπο και οι υπεύθυνοι λήψης αποφάσεων μπορεί να μην είναι σίγουροι για τις συγκρίσεις τους και μπορούν να τα αξιολογήσουν μόνο με γλωσσικούς όρους. Σε αυτό το σημείο, τα ασαφή συστήματα παρέχουν κατάλληλες τεχνικές για να μετατρέψουν τις γλωσσικές αξιολογήσεις των υπευθύνων λήψης αποφάσεων σε μια αριθμητική μορφή και να χειριστούν την αβεβαιότητα (Wang et al., 2021).

1.6 Περιβάλλον μάρκετινγκ και εσωτερικός έλεγχος

Αναπόσπαστο μέρος των βιώσιμων οικονομιών είναι το περιβάλλον μάρκετινγκ. Οι διαδικασίες προσφοράς και ζήτησης αναμειγνύονται με την υποστήριξη των σύγχρονων προσεγγίσεων μάρκετινγκ. Το περιβάλλον μάρκετινγκ διαιρείται από τους Kalieva et al. (2018) στο Μικροπεριβάλλον και στο Μακροπεριβάλλον. Ο Al-Waely (2019) περιλαμβάνει πελάτες και οργανισμούς στο Μικροπεριβάλλον, ενώ το Μακροπεριβάλλον περιλαμβάνει κυρίως το οικονομικό,

τεχνολογικό, νομικό και πολιτιστικό περιβάλλον. Οι Mose & Syaifuddin (2016) δηλώνουν στη συνέχεια σχετικά με αυτό το πρόβλημα ότι η παρακολούθηση του περιβάλλοντος μάρκετινγκ είναι στρατηγική και απαραίτητη.

Σύμφωνα με το «Ινστιτούτο Εσωτερικών Ελεγκτών (ΙΙΑ) (2020) ορίζεται η έννοια του ελέγχου ως εξής: «Ο εσωτερικός έλεγχος είναι μια ανεξάρτητη, αντικειμενική δραστηριότητα διασφάλισης και συμβουλευτικής που έχει σχεδιαστεί για να προσθέτει αξία και να βελτιώνει τις λειτουργίες ενός οργανισμού». Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013) (σελ. 3) ορίζει την έννοια του ελέγχου ως εξής: «Ο εσωτερικός έλεγχος είναι μια διαδικασία που πραγματοποιείται από το διοικητικό συμβούλιο, τη διοίκηση και το άλλο προσωπικό μιας οντότητας, σχεδιασμένη να παρέχει εύλογη βεβαιότητα σχετικά με την επίτευξη των στόχων που σχετίζονται με τις λειτουργίες, την υποβολή εκθέσεων και τη συμμόρφωση».

Η έννοια του εσωτερικού λογιστικού ελέγχου (auditing) ορίζεται κατά κύριο λόγο από την ΙΙΑ (2020) και από τους Furtuna & Ciucioi (2019), ενώ η έννοια του εσωτερικού ελέγχου (control) ορίζεται κυρίως από την COSO (2013) και από τους Lobo et. al. (2020). Ο λογιστικός έλεγχος και ο έλεγχος είναι δύο θεωρητικές έννοιες (βλ. Η1) [11]. Στην πράξη, ωστόσο, και οι δύο έννοιες μπορούν να συνδυαστούν σε μία (βλ. Η2), να οριστούν εσφαλμένα σε εννοιολογικό επίπεδο ή να συγχωνευθούν (Vachal et al., 2013).

Το χάος που προκύπτει από αυτήν την ασαφή θεωρητική θέση στη θεωρία περνάει και στην πράξη. Εάν οι έννοιες λογιστικού ελέγχου και ελέγχου συνδυάζονται σε μία σε θεωρητικό επίπεδο, μπορούν να συνδυαστούν και σε πρακτικό επίπεδο. Παρόλο που και οι δύο έννοιες μπορούν να αποκτήσουν γνώση η μία από την άλλη, θα πρέπει πάντα να εφαρμόζονται σωστά. Επομένως, οι έννοιες του λογιστικού ελέγχου θα πρέπει να εφαρμόζονται για τέτοιους σκοπούς και οι έννοιες του ελέγχου για τη διαχείριση (Kamps, 2013).

Το κείμενο στην συνέχεια εστιάζει στις έννοιες του λογιστικού ελέγχου και του ελέγχου ειδικά στο ευρωπαϊκό πλαίσιο του τρέχοντος περιβάλλοντος μάρκετινγκ των ΜΜΕ. Το περιβάλλον μάρκετινγκ είναι γεμάτο κινδύνους (Κίνδυνος επιχειρηματικών προϊόντων που μειώνουν τη ζήτηση, Κίνδυνος ατελούς εταιρικής

τιμολογιακής πολιτικής, Κίνδυνος επιχειρηματικών προϊόντων χαμηλής ποιότητας, Κίνδυνος επιχειρηματικής προώθησης πωλήσεων προϊόντων χαμηλού βαθμού) (Tkachenko et al., 2019).

Οι κίνδυνοι απειλούν αυτό το περιβάλλον και καθιστούν δύσκολη την επίτευξη των επιχειρηματικών στόχων. Για να μετριαστούν αυτοί οι κίνδυνοι, είναι απαραίτητο να χρησιμοποιηθούν οι σωστές έννοιες λογιστικού ελέγχου και έννοιες ελέγχου (οι έννοιες αντιπροσωπεύουν θεωρίες, αρχές και μοντέλα). Ο ακριβής ορισμός του λογιστικού ελέγχου και του ελέγχου, συμπεριλαμβανομένου του ιστορικού και ετυμολογικού ορισμού, είναι επομένως η βάση για την παρακάτω συζήτηση (Chornous & Ursulenko, 2013).

Το Audit βασίζεται ετυμολογικά, διαδικαστικά και εννοιολογικά στη λατινική λέξη «audire» που σημαίνει «ακούω». Ο όρος προέρχεται κυρίως από τις ιστορικές θεωρίες της Ρωμαϊκής Αυτοκρατορίας: θεωρίες για στρατιώτες, όπου οι αξιωματικοί άκουγαν τα παράπονα των στρατιωτών, θεωρίες για αξιωματούχους, όπου ο ένας άκουγε μια ανάγνωση της λογιστικής του άλλου, θεωρίες για τους διαχειριστές των οποίων οι αναφορές για τη διαχείριση ακολουθήθηκαν και θεωρίες σχετικά με τους ελεγκτές, οι οποίοι άκουγαν τους λογιστές όταν ερευνούσαν τρέχουσες πρακτικές. Η έννοια του ελέγχου βασίζεται κυρίως σε ήπιες μεθόδους επικοινωνίας (Fitriyah et al., 2020).

Ο έλεγχος (control) διαφέρει από τον λογιστικό έλεγχο ετυμολογικά, και επομένως επίσης διαδικαστικά και εννοιολογικά. Βασίζεται στα λατινικά «contra» και «rotulus» που σημαίνουν «απέναντι» και «ένας ρόλος». Η εξήγηση αυτής της έννοιας προέρχεται επίσης από ιστορικές θεωρίες: θεωρίες για υπαλλήλους που παίζουν ρόλο και ακολουθούν ένα σενάριο, θεωρίες σχετικά με λογιστές που συνδυάζουν αρχεία με πανομοιότυπα λογιστικά αρχεία, ή θεωρίες για τους ηθοποιούς, όπου κάποιος επιτρέπει ένα σενάριο και το άλλο παρακολουθεί τη συμμόρφωση ρόλων. Επομένως, η έννοια του ελέγχου βασίζεται κυρίως σε μεθόδους σκληρής σύγκρισης (Kamil & Ahmed, 2020).

Και οι δύο έννοιες ελέγχου πρέπει επίσης να ενσωματωθούν στο τρέχον περιβάλλον μάρκετινγκ. Η παγίωση της έννοιας του ελέγχου στο πλαίσιο του μάρκετινγκ σήμερα παρουσιάζεται από τους Kitchenko & Kuchina (2019), ως μελέτη

των δραστηριοτήτων μιας επιχείρησης προκειμένου να αναπτυχθεί μια πρόταση για την κατάρτιση ενός σχεδίου δράσης με στόχο την αύξηση της αποτελεσματικότητας του μάρκετινγκ της επιχείρησης. Αντίθετα, ο έλεγχος στο πλαίσιο του μάρκετινγκ ορίζεται σήμερα ως παρακολούθηση, κατεύθυνση και αξιολόγηση για να διασφαλιστεί ότι το σχέδιο μάρκετινγκ εφαρμόζεται όπως έχει οραματιστεί και, όταν αυτό δεν συμβαίνει, λαμβάνεται διορθωτική δράση (Brown & Crosno, 2019).

1.7 Η σημασία του εσωτερικού ελέγχου στις συλλογικές διαπραγματεύσεις

Οι χρηματοοικονομικές πληροφορίες συχνά διαδραματίζουν σημαντικό ρόλο στις συλλογικές διαπραγματεύσεις μεταξύ των ενδιαφερόμενων φορέων. Για παράδειγμα, όταν μια επιχείρηση αντιμετωπίζει υψηλή κερδοφορία, τα συνδικάτα υποστηρίζουν συχνά ότι η επιχείρηση μπορεί να αντέξει οικονομικά αυξήσεις αποζημίωσης. Επίσης, όταν η διοίκηση υποστηρίζει ότι η επιχείρηση δεν είναι σε θέση να ανταποκριθεί στις απαιτήσεις ενός συνδικάτου, οι οικονομικές πληροφορίες χρησιμοποιούνται για την αξιολόγηση της αλήθειας αυτού του ισχυρισμού (Carrell & Heavrin, 2009).

Οι λογιστικές πληροφορίες αναφέρονται επίσης συχνά από εκπροσώπους των συνδικάτων για να δικαιολογήσουν την αποδοχή ή την απόρριψη μιας πρότασης. Ωστόσο, ακόμη και όταν η ικανότητα της επιχείρησης να πληρώσει για τις απαιτήσεις ενός συνδικάτου δεν είναι ρητά θέμα διαπραγμάτευσης, η οικονομική κατάσταση της επιχείρησης συχνά διαμορφώνει την πορεία των διαπραγματεύσεων (Brown, 2000).

Για παράδειγμα, ο Brown (2000) σημειώνει ότι ακόμη και όταν το επίκεντρο των διαπραγματεύσεων είναι σε άλλους παράγοντες εκτός από την κερδοφορία, η ικανότητα πληρωμής μπορεί να είναι σημαντική ως βασικός ψυχολογικός παράγοντας, καθώς μπορεί να βοηθήσει στον καθορισμό των ορίων διαπραγμάτευσης. Τα συνδικάτα μπορεί, για παράδειγμα, να αποτύχουν να προωθήσουν μια αξίωση από φόβο ότι οι οικονομικές πιέσεις θα οδηγήσουν σε απολύσεις (Brown, 2000). Παρά τον σημαντικό ρόλο των οικονομικών πληροφοριών

στις διαπραγματεύσεις, τα συνδικάτα πρέπει συχνά να βασίζονται σε δημοσιευμένες οικονομικές εκθέσεις, επειδή οι διευθυντές γενικά δεν απαιτείται να παρέχουν στα συνδικάτα οικονομικές πληροφορίες (Brown, 2000).

Δεδομένης της σημασίας των οικονομικών πληροφοριών στις συλλογικές διαπραγματεύσεις, τα συνδικάτα έχουν λόγους να απαιτούν υψηλής ποιότητας χρηματοοικονομικές πληροφορίες. Προηγούμενες μελέτες υποστήριξαν ότι όταν τα συνδικάτα είναι πιο ενημερωμένα, είναι σε θέση να λάβουν μεγαλύτερη αποζημίωση λόγω της ικανότητάς τους να διαπραγματεύονται πιο επιδέξια (Cheng, 2011).

Υποστηρίζοντας αυτή την ιδέα, οι Kleiner & Bouillon (1988) βρίσκουν ότι τα συνδικάτα λαμβάνουν υψηλότερους μισθούς όταν τους παρέχονται οικονομικές πληροφορίες από τη διοίκηση. Ως εκ τούτου, στο βαθμό που οι οικονομικές πληροφορίες υψηλής ποιότητας είναι πιο ενημερωτικές, ωφελούν τα συνδικάτα μειώνοντας την ασυμμετρία πληροφόρησης και διευκολύνοντας την αύξηση των απολαβών τους.

Δεδομένου ότι τα συνδικάτα μπορούν να επωφεληθούν από υψηλότερης ποιότητας χρηματοοικονομικές πληροφορίες, έχουν επίσης λόγους να απαιτούν ένα ισχυρό σύστημα εσωτερικού ελέγχου. Οι ελεγκτές οφείλουν να ελέγχουν το σύστημα εσωτερικού ελέγχου μιας επιχείρησης επί της χρηματοοικονομικής αναφοράς και να εκδίδουν γνώμη για την αποτελεσματικότητά του. Το Ελεγκτικό Πρότυπο No. 5 ορίζει μια σημαντική αδυναμία ως εξής:

«Μια ουσιώδης αδυναμία είναι μια ανεπάρκεια ή ένας συνδυασμός ελλείψεων στον εσωτερικό έλεγχο της χρηματοοικονομικής πληροφόρησης, έτσι ώστε να υπάρχει εύλογη πιθανότητα να μην αποτραπεί ή να εντοπιστεί ουσιώδης ανακρίβεια των ετήσιων ή ενδιάμεσων οικονομικών καταστάσεων της εταιρείας» (PCAOB, 2007).

Τα συνδικάτα είναι πιθανό να ενδιαφέρονται για την ποιότητα του εσωτερικού ελέγχου για διάφορους λόγους. Πρώτον, οι υλικές αδυναμίες συνδέονται με χαμηλότερη ποιότητα αποδοχών υπονοώντας κέρδη που είναι λιγότερο ανάλογα των δηλωθέντων . Δεύτερον, προηγούμενες μελέτες δείχνουν ότι ο ασθενής εσωτερικός έλεγχος δημιουργεί μεγαλύτερη αβεβαιότητα στα κέρδη.

Για παράδειγμα, η υπάρχουσα έρευνα διαπιστώνει ότι οι ουσιώδεις αδυναμίες συνδέονται με μεγαλύτερα σφάλματα προβλέψεων και διασπορά προβλέψεων των αναλυτών (Clinton et al., 2014), υποδηλώνοντας ότι ο ανεπαρκής εσωτερικός έλεγχος δημιουργεί θόρυβο στη μέτρηση των κερδών. Υποστηρίζοντας αυτή την άποψη, οι Ashbaugh-Skaife et al. (2008) διαπιστώνουν ότι η αρνητική συσχέτιση μεταξύ των υλικών αδυναμιών και της ποιότητας των κερδών αποδίδεται σε «ακούσια σφάλματα που προσθέτουν θόρυβο στα δεδουλευμένα».

Για αυτούς τους λόγους, ο αδύναμος εσωτερικός έλεγχος πιθανότατα καθιστά πιο δύσκολη την αποτελεσματική ερμηνεία και αποτελεσματική χρήση των κερδών από τα συνδικάτα. Τέλος, επειδή ο ισχυρός εσωτερικός έλεγχος αυξάνει την ποιότητα των οικονομικών πληροφοριών πριν από τον έλεγχο, τα συνδικάτα επωφελούνται από ισχυρό εσωτερικό έλεγχο εάν η διοίκηση τους παρέχει οικονομικές πληροφορίες του τρέχοντος έτους που δεν έχουν ακόμη ελεγχθεί.

Από την άλλη πλευρά, προηγούμενη έρευνα υποδηλώνει ότι ο ασθενής εσωτερικός έλεγχος παρέχει στους διευθυντές μεγαλύτερη ευκαιρία να χειραγωγήσουν τις οικονομικές πληροφορίες. Η ιδέα ότι ο αδύναμος εσωτερικός έλεγχος μπορεί να διευκολύνει τη χειραγώγηση της διοίκησης έχει εκφραστεί σε προηγούμενη έρευνα (π.χ. Donelson et al., 2014) καθώς και στα Πρότυπα Ελέγχου No. 2 (PCAOB, 2004).) και No. 5 (PCAOB, 2007).

Για παράδειγμα, οι Skaife et al. (2013) αναφέρουν ότι όταν οι εταιρείες έχουν αναποτελεσματικό εσωτερικό έλεγχο επί της χρηματοοικονομικής αναφοράς, οι διευθυντές έχουν μεγαλύτερη διακριτική ευχέρεια όσον αφορά τις λογιστικές εκτιμήσεις και τις μεθόδους λόγω της έλλειψης επίσημων πολιτικών και διαδικασιών που περιορίζουν τις λογιστικές επιλογές των διευθυντών.

Περαιτέρω, σύμφωνα με το Ελεγκτικό Πρότυπο No. 2, «πολλές απάτες που είχαν ως αποτέλεσμα την επαναδιατύπωση των οικονομικών καταστάσεων βασίστηκαν στην ικανότητα της διοίκησης να εκμεταλλευτεί αδυναμίες στον εσωτερικό έλεγχο» (PCAOB, 2004). Σύμφωνα με αυτή την αντίληψη, οι Chan et al. (2008) βρήκαν μια θετική συσχέτιση μεταξύ ουσιωδών αδυναμιών και διαχείρισης κερδών. Επίσης, οι Donelson et al. (2014) διαπιστώνουν ότι οι ουσιώδεις αδυναμίες συνδέονται με μελλοντικές ανακοινώσεις απάτης και οι συγγραφείς παρέχουν

στοιχεία ότι αυτή η συσχέτιση αποδίδεται σε ανεπαρκή εσωτερικό έλεγχο που δημιουργεί ευκαιρίες για χειραγώγηση.

Επιπλέον, οι Skaife et al. (2013) υποστηρίζουν ότι ο ανεπαρκής εσωτερικός έλεγχος αυξάνει την ασυμμετρία πληροφοριών. Σύμφωνα με αυτήν την υπόθεση, οι συγγραφείς διαπιστώνουν ότι οι υλικές αδυναμίες συνδέονται με πιο κερδοφόρες συναλλαγές από τιε εμπιστευτικές πληροφορίες (Skaife et al., 2013).

Ως εκ τούτου, δεδομένου του διοικητικού κινήτρου για τη διατήρηση ενός πληροφοριακού πλεονεκτήματος έναντι των συνδικάτων, οι διευθυντές μπορεί να προτιμούν ασθενέστερο εσωτερικό έλεγχο επειδή αυτός

(1) παρέχει στους διευθυντές μεγαλύτερη ικανότητα χειραγώγησης οικονομικών πληροφοριών και

(2) προάγει την ασυμμετρία πληροφοριών.

Δεδομένου ότι η αποκάλυψη μιας υλικής αδυναμίας μπορεί να επιβάλει κόστος στην επιχείρηση, οι διευθυντές είναι απίθανο να διατηρήσουν σκόπιμα ένα σύστημα εσωτερικού ελέγχου που έχει ουσιώδη αδυναμία. Ωστόσο, όλα τα άλλα, οι διευθυντές των συνδικαλιστικών εταιρειών έχουν λόγους να προτιμούν σχετικά ασθενέστερα συστήματα εσωτερικού ελέγχου, τα οποία, με τη σειρά τους, μπορεί να κάνουν τις συνδικαλιστικές ενώσεις πιο πιθανό να αναφέρουν μια ουσιώδη αδυναμία. Ως εκ τούτου, για τους προαναφερθέντες λόγους, είναι αβέβαιο εάν η ισχύς της ένωσης οδηγεί σε υψηλότερη ή χαμηλότερη ποιότητα εσωτερικού ελέγχου.

2. Η σημασία του εσωτερικού ελέγχου στους οργανισμούς παροχής υπηρεσιών υγείας

2.1. Η ειδική σημασία του ελέγχου στους οργανισμούς παροχής υπηρεσιών υγείας

Η ασφάλεια των ασθενών θα πρέπει να είναι η κορυφαία προτεραιότητα κάθε συμβουλίου νοσοκομείων. Τα συμβούλια των νοσοκομείων είναι νομικά υπεύθυνα για την ποιότητα και την ασφάλεια της παρεχόμενης φροντίδας σε αυτά. Ωστόσο, ενώ η ανάγκη για επίβλεψη ασφάλειας του συμβουλίου αυξάνεται, η υγειονομική περίθαλψη εξακολουθεί να είναι συχνά μη ασφαλής και τα συμβούλια αντιμετωπίζουν δυσκολίες στην επίβλεψη των κινδύνων ασφάλειας. Για να εκπληρώσουν τον ρόλο διακυβέρνησής τους, τα συμβούλια των νοσοκομείων χρειάζονται μεθόδους και εργαλεία που παρέχουν πληροφορίες παρακολούθησης για τον μετριασμό ή την πρόληψη ανεπιθύμητων συμβάντων (Glazebrook & Buchanan, 2001).

Υπάρχουν διάφορες πηγές για τη συλλογή πληροφοριών που βοηθούν τα συμβούλια με τη διακυβέρνηση της ασφάλειας των ασθενών και οι πληροφορίες από εσωτερικούς ελέγχους μπορεί να είναι μία από αυτές. Ο εσωτερικός έλεγχος είναι ένα «αντικειμενικό σύστημα διασφάλισης και συμβουλευτικής για την έγκαιρη ανίχνευση των κινδύνων ανεπιθύμητων ενεργειών των ασθενών», το οποίο «θα πρέπει να ενθαρρύνει τη συνεχή βελτίωση της ασφάλειας των ασθενών» (Ivers et al., 2012).

Είναι μια συστηματική αξιολόγηση του συστήματος ποιότητας ενός νοσοκομείου που στοχεύει να βελτιώσει την ασφάλεια των ασθενών μετρώντας την απόδοση των παρόχων υγειονομικής περίθαλψης και τις προϋποθέσεις για ασφαλή φροντίδα και συγκρίνοντας αυτά τα αποτελέσματα με (εθνικά) πρότυπα και κατευθυντήριες γραμμές. Οι μετρήσεις εκτελούνται από μια ομάδα ελέγχου που αποτελείται από εσωτερικούς συναδέλφους (δηλαδή, υπαλλήλους ενός νοσοκομείου που ελέγχουν συναδέλφους άλλων τμημάτων). Η μέθοδος εφαρμόστηκε τη δεκαετία

του 1990 για να μετρηθεί εάν υπάρχουν οργανωτικές προϋποθέσεις για ασφαλή φροντίδα και για να προκληθούν βελτιώσεις όταν εντοπίζονται προβλήματα ασφάλειας. Οι εσωτερικοί έλεγχοι ξεκινούν από τα συμβούλια των νοσοκομείων και εφαρμόζονται από πάνω προς τα κάτω (Hanskamp et al., 2013).

Έχουν διεξαχθεί αρκετές μελέτες σχετικά με την αποτελεσματικότητα των κλινικών ελέγχων στην επαγγελματική πρακτική. Τα αποτελέσματα που βρέθηκαν είναι λίγα και διαφέρουν ανά μελέτη. Αυτό μπορεί να εξηγηθεί εν μέρει από τις διαφορές στον πληθυσμό της μελέτης, τη μορφή και το περιεχόμενο των μελετημένων ελέγχων και τις χρησιμοποιούμενες ερευνητικές μεθόδους και τα αποτελέσματα. Ωστόσο, η γνώση σχετικά με την αποτελεσματικότητα των εσωτερικών ελέγχων για τη διακυβέρνηση της εσωτερικής ασφάλειας των ασθενών από τα διοικητικά συμβούλια των νοσοκομείων είναι σπάνια (Wagner et al., 2006).

Ο λόγος που σχεδόν όλα τα ευρωπαϊκά νοσοκομεία χρησιμοποιούν εσωτερικούς ελέγχους για σκοπούς διακυβέρνησης είναι ένας συνδυασμός νομικών και ηθικών υποχρεώσεών τους απέναντι στην κοινότητα. Τα νοσοκομεία υποχρεούνται από τον νόμο περί ποιότητας των ιδρυμάτων περίθαλψης να διαθέτουν ένα σύστημα διαχείρισης ποιότητας, συμπεριλαμβανομένης της διασφάλισης ότι αναλαμβάνονται δραστηριότητες ποιότητας.19 Από τη δεκαετία του 1990, πολλά νοσοκομεία χρησιμοποιούν διάφορα πρότυπα διασφάλισης ποιότητας (van Gennip & Smitt, 2010).

Προκειμένου να διαπιστευθούν διάφορα ινστιτούτα ποιότητας και για να παρέχεται η διασφάλιση της ασφαλούς φροντίδας σε τρίτους (π.χ. καταναλωτές υγειονομικής περίθαλψης και ασφαλιστές υγειονομικής περίθαλψης), θα πρέπει να υπάρχει ένα σύστημα εσωτερικού ελέγχου, καθώς τα εξωτερικά μέρη διαπίστευσης έχουν τους δικούς τους ελέγχους που τους πραγματοποιούν για να δουν εάν ένα νοσοκομείο είναι έτοιμο για εξωτερική διαπίστευση (Secanell et al., 2014).

2.2. Τύποι ελέγχων στους οργανισμούς παροχής υπηρεσιών υγείας

Τα τελευταία χρόνια, τα θέματα ποιότητας και ασφάλειας έχουν γίνει ολοένα και πιο σημαντικά στη νοσοκομειακή περίθαλψη μετά από αυξημένη εστίαση τόσο στα κλινικά αποτελέσματα όσο και στην ικανοποίηση των ασθενών. Οι υγειονομικές αρχές και οι οργανισμοί δίνουν προτεραιότητα στους ελέγχους ως προσέγγιση βελτίωσης της ποιότητας (quality improvement, QI) με τη συστηματική αξιολόγηση της παρεχόμενης φροντίδας, τον εντοπισμό περιοχών για βελτίωση και την εφαρμογή αλλαγών προς το καλύτερο (Spencer & Walshe, 2009).

Διάφοροι τύποι ελέγχων, συμπεριλαμβανομένων των εξωτερικών ελέγχων, των εσωτερικών ελέγχων, των αξιολογήσεων από ομοτίμους και των κλινικών ελέγχων, έχουν χρησιμοποιηθεί, αλλά όλοι μοιράζονται το πρόβλημα ότι η εφαρμογή των προτεινόμενων βελτιώσεων συχνά αποτυγχάνει να καλύψει το κενό ποιότητας που αυτοί σημείωσαν. Η περιορισμένη αποτελεσματικότητα των ελέγχων υποδηλώνει ότι η διεξαγωγή ελέγχων και η εφαρμογή βελτιώσεων δεν είναι μια απλή διαδικασία. Παρόλο που έχουν προσφερθεί διάφορες εξηγήσεις για τον τρόπο λειτουργίας των ελέγχων, έχει υπάρξει ελάχιστη σε βάθος θεωρία σχετικά με τους αιτιώδεις μηχανισμούς που καθορίζουν την αποτελεσματικότητα των ελέγχων σε ένα δεδομένο πλαίσιο (Kaplan et al., 2010).

Οι έλεγχοι που χρησιμοποιούνται στον τομέα της βελτίωσης της υγειονομικής περίθαλψης μπορούν χονδρικά να χωριστούν σε (Bohigas & Heaton, 2000):

(1) εξωτερικούς ελέγχους, που χρησιμοποιούνται για την απόκτηση εικόνας σχετικά με τη συμμόρφωση ενός νοσοκομείου με εξωτερικά κριτήρια (π.χ. διαπίστευση, πιστοποίηση, εξωτερικές αξιολογήσεις από ομοτίμους).

(2) εσωτερικούς ελέγχους, συχνά στο πλαίσιο προετοιμασίας για εξωτερικό έλεγχο και

(3) κλινικοί έλεγχοι, που πραγματοποιούνται ως τοπική πρωτοβουλία από επαγγελματίες υγείας.

Αν και υπάρχουν διαφορές ως προς το εύρος και τις προσεγγίσεις που χρησιμοποιούνται στους ελέγχους, όλοι μοιράζονται τον στόχο της βελτίωσης της ποιότητας της νοσοκομειακής περίθαλψης (Bohigas & Heaton, 2000). Στην συνέχεια,

παρουσιάζονται οι βασικοί τύποι ελέγχων στους οργανισμούς παροχής υπηρεσιών υγείας.

Εξωτερικά καθοδηγούμενοι έλεγχοι. Για παράδειγμα, η διαπίστευση, η πιστοποίηση και οι εξωτερικές αξιολογήσεις από ομοτίμους έχουν εδραιωθεί έντονα στη διασφάλιση ποιότητας (quality assurance, QA), αναφερόμενοι σε πρωτοβουλίες που έχουν σχεδιαστεί για να διασφαλίζουν τη συμμόρφωση με ελάχιστα πρότυπα ποιότητας. Η διασφάλιση ποιότητας ορίζεται ως: «Το μέρος της διαχείρισης ποιότητας που επικεντρώνεται στην παροχή εμπιστοσύνης ότι οι απαιτήσεις ποιότητας θα εκπληρωθούν ». Οι εξωτερικοί έλεγχοι χρησιμοποιούνται για την αξιολόγηση του συστήματος ποιότητας ενός οργανισμού υγειονομικής περίθαλψης με βάση καθορισμένα πρότυπα και διενεργούνται από εξωτερικούς ελεγκτές (Walshe et al., 2000).

Εσωτερικοί έλεγχοι. Αυτός ο τύπος ελέγχου διενεργείται από εσωτερικούς ελεγκτές του οργανισμού του ίδιου του νοσοκομείου, όπως αξιωματούχους ποιότητας ή επαγγελματίες υγείας από άλλο τμήμα από αυτό που ελέγχεται, ώστε να διασφαλίζεται η ανεξάρτητη κρίση. Οι εσωτερικοί έλεγχοι χρησιμοποιούνται επίσης για την αξιολόγηση του συστήματος ποιότητας βάσει προτύπων. Διενεργούνται για την προετοιμασία για εξωτερικούς ελέγχους. Οι οργανισμοί υγειονομικής περίθαλψης χρησιμοποιούν επίσης εσωτερικούς ελέγχους για τη συνεχή βελτίωση της ποιότητας της υγειονομικής περίθαλψης. Οι εσωτερικοί έλεγχοι έχουν σχεδιαστεί για να αξιολογούν και να βελτιώνουν την αποτελεσματικότητα του συστήματος διαχείρισης ποιότητας του οργανισμού και να εστιάζουν περισσότερο στις οργανωτικές συνθήκες παρά στην απόδοση των επαγγελματιών υγείας και στα αποτελέσματα των ασθενών (Bohigas & Heaton, 2000).

Κλινικοί έλεγχοι. Οι κλινικοί έλεγχοι διαφέρουν από άλλους τύπους ελέγχων στο ότι ως επί το πλείστον ξεκινούν και αναλαμβάνονται από επαγγελματίες του τομέα της υγείας. Οι κλινικοί έλεγχοι αντιπροσωπεύουν μια στροφή από το QA στο QI, με έμφαση στην αύξηση της ικανότητας εκπλήρωσης των απαιτήσεων ποιότητας, επιδιώκοντας τη βελτίωση της φροντίδας, τη βελτίωση της απόδοσης και την πρόληψη της κακής φροντίδας. Αυτή η διαδικασία λαμβάνει χώρα συνεχώς ως μέρος της καθημερινής ρουτίνας, καθώς οι επαγγελματίες υγείας συνεργάζονται για τη συλλογή δεδομένων και την αξιολόγηση των δικών τους πρακτικών. Μετά από αυτό,

σκοπεύουν να αναπτύξουν και να εφαρμόσουν βελτιώσεις στην καθημερινή πρακτική, και στη συνέχεια ο κύκλος ελέγχου επαναλαμβάνεται για να επιδείξει βελτιωμένες πρακτικές και συνεχείς βελτιώσεις. Ως εκ τούτου, οι κλινικοί έλεγχοι δεν χρησιμοποιούν απαραίτητα εξωτερικά κριτήρια και δεν πραγματοποιούνται ως απάντηση σε εξωτερικές απαιτήσεις, καθώς η πρωτοβουλία προέρχεται από τους ίδιους τους επαγγελματίες υγείας (Dixon, 2007).

Εξάλλου, όπως σημειώθηκε και πριν, Βασική ευθύνη ενός οργανισμού είναι η απόκτηση διαβεβαίωσης ότι οι σημαντικοί κίνδυνοι για την επίτευξη των στρατηγικών στόχων του αντιμετωπίζονται αποτελεσματικά. Η διασφάλιση κινδύνου σε επίπεδο συμβουλίου επιτυγχάνεται μέσω ποικίλων μηχανισμών, συμπεριλαμβανομένων των εκθέσεων διαχείρισης και επιτροπών, εξωτερικών ελέγχων και εσωτερικών ελέγχων.

Ο εσωτερικός έλεγχος έχει οριστεί ως «μια ανεξάρτητη, αντικειμενική δραστηριότητα διασφάλισης και συμβουλευτικής που έχει σχεδιαστεί για να προσθέτει αξία και να βελτιώνει τις λειτουργίες ενός οργανισμού». Οι εσωτερικοί έλεγχοι σε οργανισμούς υγειονομικής περίθαλψης έχουν χρησιμοποιηθεί ευρέως για την παροχή διαβεβαίωσης στα συμβούλια σχετικά με την ευρωστία των διαφόρων οικονομικών ελέγχων που ισχύουν για τη διαχείριση των οικονομικών κινδύνων και τη διασφάλιση της επίτευξης των οικονομικών στόχων (IIA, 2011).

Θεωρητικά, οι βέλτιστες πρακτικές προσεγγίσεις εσωτερικού ελέγχου θα πρέπει να «κατευθύνουν τις δραστηριότητές τους στους πιο σημαντικούς κινδύνους της οντότητας και στους ελέγχους που υπάρχουν για τη διαχείρισή τους». Είναι καλά τεκμηριωμένο στη βιβλιογραφία ότι οι παρεμβάσεις υγειονομικής περίθαλψης φέρουν σημαντικούς κινδύνους για τους ασθενείς και τους καταναλωτές. Οι ασθενείς έχουν «μία στις δύο πιθανότητες να λάβουν τη σωστή φροντίδα, πιθανότητα 1:10 να υποστούν βλάβη σε συνδυασμό με εισαγωγή στο νοσοκομείο και 1:50 πιθανότητα θανάτου ή μείζονος αναπηρίας από το σύστημα». Είναι λογικό τότε το συμβούλιο να χαιρετίζει παρόμοιο βαθμό διασφάλισης όσον αφορά τη διαχείριση του κλινικού κινδύνου με τον οικονομικό κίνδυνο (Braithwaite & Coiera, 2010).

Οι εσωτερικοί έλεγχοι των κλινικών περιοχών διαφέρουν από τους κλινικούς ελέγχους. Οι κλινικοί έλεγχοι γενικά διευθύνονται από το προσωπικό της περιοχής

του προγράμματος και μπορεί να σχετίζονται μόνο με σημαντικούς κινδύνους. Τα αποτελέσματα των κλινικών ελέγχων συχνά παραδίδονται σε επιτροπές ποιότητας ή διαχειριστές περιοχών. Αντίθετα, ο εσωτερικός έλεγχος μιας κλινικής περιοχής βασίζεται στην αξιολόγηση σημαντικών κινδύνων για τον οργανισμό, που διενεργείται ανεξάρτητα από διαπιστευμένους εσωτερικούς ελεγκτές σύμφωνα με τα διεθνή πρότυπα εσωτερικού ελέγχου και τα αντικειμενικά ευρήματα αναφέρονται σε μια επιτροπή ελέγχου. Οι εσωτερικοί έλεγχοι περιγράφονται συχνά ως η τρίτη γραμμή άμυνας στη διαχείριση κινδύνου, με την πρώτη γραμμή να είναι οι καθημερινοί επιχειρησιακοί έλεγχοι και οι διαδικασίες για την καθοδήγηση της φροντίδας και της διαχείρισης του κινδύνου σε κάθε τομέα του οργανισμού και η δεύτερη γραμμή άμυνα είναι οι λειτουργίες διαχείρισης κινδύνου και συμμόρφωσης σε επίπεδο οργανισμού (IIA, 2013).

Η προσοχή που δόθηκε στην κλινική διακυβέρνηση τις τελευταίες δύο δεκαετίες ως απάντηση στις αποτυχίες υψηλού προφίλ ασφάλειας και ποιότητας στην υγειονομική περίθαλψη έχει τονίσει τις απαιτήσεις των υγειονομικών επιτροπών για «παρακολούθηση της ασφάλειας των ασθενών με την ίδια αυστηρότητα και προσοχή που δίνουν στην εταιρική και οικονομική απόδοση» (Victorian Auditor-General's Office, 2005).

Ενώ η επέκταση της μεθοδολογίας εσωτερικού ελέγχου στον κλινικό τομέα είναι θεωρητικά λογική, υπάρχουν ελάχιστα στοιχεία για την εφαρμογή της στους κλινικούς τομείς μέχρι σήμερα. Φαίνεται ότι το κύριο εμπόδιο για την ευρεία χρήση του εσωτερικού ελέγχου σε κλινικούς τομείς είναι η έλλειψη υφιστάμενων κατευθυντήριων γραμμών, εργαλείων εσωτερικού ελέγχου σε αυτόν τον τομέα και η διαθεσιμότητα των διαπιστευτηρίων συνδυασμένου ελέγχου και κλινικής εμπειρογνωμοσύνης που απαιτούνται για τη διενέργεια εσωτερικού ελέγχου μιας κλινικής περιοχής (Victorian Auditor-General's Office, 2005).

2.3 Η σύνδεση του εσωτερικού ελέγχου των μονάδων υγείας με το Σύστημα Διαχείρισης Ποιότητας

Από την καθιέρωση της έννοιας του ελέγχου, οι ερευνητές βρίσκονται αντιμέτωποι με διαφορετικούς ορισμούς που προσπαθούν να προσδιορίσουν λίγο πολύ τη φύση του ελέγχου. Ο Lee (1984) όρισε τον έλεγχο ως έναν τρόπο με τον οποίο ο ελεγκτής διαβεβαιώνει τον ελεγχόμενο για την ποιότητα, και την κατάσταση του θέματος που εξετάστηκε από τον ελεγκτή. Η ανάγκη για έναν τέτοιο έλεγχο προκύπτει επειδή ο ελεγχόμενος έχει αμφιβολίες ή δεν είναι σίγουρος για την ποιότητα ή την κατάσταση του θέματος και δεν είναι σε θέση να απαλλαγεί από αυτές τις αμφιβολίες ή αβεβαιότητες.

Η Silvoso (1972) αντιλαμβάνεται τον έλεγχο ως μια συστηματική διαδικασία αντικειμενικής απόκτησης και αξιολόγησης στοιχείων σχετικά με τις πληροφορίες για οικονομικές δραστηριότητες και γεγονότα προκειμένου να καθοριστεί το μέτρο συμφωνίας με τα καθιερωμένα κριτήρια και να κοινοποιηθούν τα αποτελέσματα στους ενδιαφερόμενους.

Οι Arens et al. (2003) ισχυρίζονται ότι ο έλεγχος είναι η συλλογή αποδεικτικών στοιχείων και η αξιολόγηση πληροφοριών με σκοπό τον προσδιορισμό και την αναφορά του βαθμού συσχέτισης μεταξύ των πληροφοριών που συλλέγονται και των κριτηρίων που έχουν καθοριστεί. Ο έλεγχος θα πρέπει να διενεργείται από ικανό και ανεξάρτητο άτομο.

Ακολουθεί ο ορισμός του ελέγχου με βάση την αποσπασματική γνώση του εγχώριου θεωρητικού υπόβαθρου σύμφωνα με τον νόμο αριθ. 540/2007 Συντ. σχετικά με τους ελεγκτές, τον έλεγχο και την εποπτεία ελέγχου: ο έλεγχος είναι η επαλήθευση των μεμονωμένων οικονομικών καταστάσεων ή των ενοποιημένων οικονομικών καταστάσεων και η επαλήθευση συμμόρφωσης της ατομικής ετήσιας έκθεσης με τις ατομικές οικονομικές καταστάσεις ή η επαλήθευση συμμόρφωσης της ενοποιημένης ετήσιας έκθεσης με την ενοποιημένη ετήσια έκθεση (Kares, 2010).

Ο Kares ορίζει τον έλεγχο ως δραστηριότητα τον έλεγχο, που μπορεί να χαρακτηριστεί ως εξειδικευμένο επάγγελμα, προσανατολισμένο στην πολυμερή και ολοκληρωμένη εξέταση και ειδική αξιολόγηση μιας εταιρείας. Η εταιρεία θεωρείται ως ένα δυναμικό αντικείμενο με σαφές συμπέρασμα ελέγχου σχετικά με τον σκοπό για τον οποίο παραγγέλθηκε. Ο σκοπός διατυπώθηκε από τον πελάτη και ο ελεγκτής αναλαμβάνει να του παράσχει έγκυρα συμπεράσματα για τη λήψη αποφάσεων. Οι

ορισμοί του ελέγχου ποικίλλουν ανάλογα με το περιεχόμενο και τον προσανατολισμό, π.χ. Ο οικονομικός έλεγχος διαφέρει από τον έλεγχο της νοσηλευτικής περίθαλψης.

Όσον αφορά τη νοσηλευτική φροντίδα, οι Farkasovs et al. (2001) όρισαν έναν έλεγχο ως τη συστηματική αξιολόγηση της ποιότητας της νοσηλευτικής περίθαλψης σε σχέση με την αποτελεσματικότητά της, τη σχέση κόστους-αποτελεσματικότητας και την ηθική της επάρκεια. Είναι μια βασική τεχνική για την ανίχνευση της ποιότητας. Αυτή η έννοια του ελέγχου είναι το σημείο εκκίνησης για τη μοντελοποίηση της διαδικασίας εσωτερικού ελέγχου στις εγκαταστάσεις υγειονομικής περίθαλψης.

Αναμφίβολα, μπορούμε να ορίσουμε με σαφήνεια τη στοιχειώδη ουσία του ορισμού του ελέγχου, δηλαδή ότι πρόκειται για μια συστηματική αξιολόγηση του ελεγχόμενου θέματος που βασίζεται σε προκαθορισμένους κανόνες, τύπους και πρότυπα για την περιοχή. Ο έλεγχος όσον αφορά τη διαχείριση ποιότητας ορίζεται ως μια συστηματική, ανεξάρτητη και τεκμηριωμένη διαδικασία για τη συγκέντρωση ελεγκτικών τεκμηρίων και την αντικειμενική αξιολόγησή τους, προκειμένου να καθοριστεί ο βαθμός στον οποίο πληρούνται τα κριτήρια ελέγχου (Emark, 2000).

Η ποιότητα ενός ελέγχου είναι ένα εργαλείο που βοηθά όχι μόνο στη βελτίωση της ποιότητας, αλλά και στη μείωση του κόστους. Μπορεί να οριστεί ως μια συστηματική και ανεξάρτητη εξέταση για να καθοριστεί εάν οι ποιοτικές δραστηριότητες και τα σχετικά αποτελέσματα συνάδουν με τον επιδιωκόμενο σκοπό και εάν αυτά τα σχέδια εφαρμόστηκαν αποτελεσματικά και είναι κατάλληλα για την επίτευξη συγκεκριμένων στόχων.

Ο όρος «σύστημα διαχείρισης ποιότητας» σημαίνει μια οργανωτική δομή, διαδικασίες και πόρους που είναι απαραίτητοι για την εφαρμογή της διαχείρισης ποιότητας. Σημαντικό ορόσημο στην ανάπτυξη της διαχείρισης ποιότητας ήταν η δημοσίευση του ISO 9000 το 1987 από τον Διεθνή Οργανισμό Τυποποίησης. Το πρότυπο σηματοδότησε την αρχή ενός «ταξιδιού προς την αριστεία» και ήταν ένα αποτελεσματικό μέσο για τη βελτίωση της εργασίας εντός του οργανισμού (Mateides & Dado, 2002).

Δεν ασχολήθηκε με τις τεχνικές απαιτήσεις για την παραγωγή και τις διεργασίες, αλλά μόνο τις απαιτήσεις συστήματος και για αυτό ονομάστηκε Σύστημα Διαχείρισης Ποιότητας (Quality Management System, QMS). Το QMS αποτελείται από πραγματικά σαφείς οδηγίες για τη συμπεριφορά της ποιότητας του οργανισμού. Σε αυτό το πλαίσιο, η λέξη ποιότητα δεν σημαίνει καλή ή καλύτερη κατάσταση, αλλά είναι η ικανότητα του οργανισμού να ανταποκρίνεται στις ανάγκες των πελατών (Mateides & Dado, 2002).

Είναι σημαντικό να σημειωθεί ότι στις μέρες μας, η ποιότητα του συστήματος διαχείρισης δεν αποτελεί πολυτέλεια, αλλά αναγκαιότητα για τη διασφάλιση μακροπρόθεσμης ανταγωνιστικότητας. Η προηγούμενη προσέγγιση της διαχείρισης ποιότητας με τη μορφή ελέγχων σε προϊόντα ή υπηρεσίες έχει σήμερα αλλάξει σε απαιτούμενη προσέγγιση συστημάτων. Ο όρος ποιότητα σημαίνει ένα σύνολο χαρακτηριστικών που καθορίζουν τον βαθμό (επίπεδο) του προϊόντος, και αντίστοιχα υπηρεσίες για την κάλυψη των αναγκών του αποδέκτη (Gubova, 2013).

Οι έλεγχοι ποιότητας έχουν γίνει ουσιαστικό μέρος της πολιτικής ποιότητας. Η παροχή ποιοτικών υπηρεσιών σε εγκαταστάσεις υγείας διασφαλίζει τα καλύτερα δυνατά εφικτά πρότυπα για την υγειονομική περίθαλψη. Σε πολλές χώρες υπάρχουν νόμου περί των υπηρεσιών υγείας και των όρων παροχής τους με στόχο να αξιολογούνται τα καθήκοντα του παρόχου για τη δημιουργία ενός εσωτερικού συστήματος αξιολόγησης της ποιότητας και της ασφάλειας των παρεχόμενων υπηρεσιών υγείας (Gubova, 2013).

Η διαχείριση της ποιότητας στις εγκαταστάσεις υγειονομικής περίθαλψης είναι αναμφίβολα πολύ πιο περίπλοκη στον χώρο της υγείας από ό, τι στη βιομηχανία. Προέρχεται από μια διαφορετική κατανόηση της ποιότητας και της πολυπλοκότητας του οργανωτικού συστήματος των εγκαταστάσεων υγειονομικής περίθαλψης. Ποιότητα υπηρεσιών υγείας σημαίνει όχι μόνο υψηλή υλικοτεχνική παροχή του χώρου εργασίας, αλλά και ανθρώπινη πρόσβαση όλου του προσωπικού υγειονομικής περίθαλψης στους πελάτες. Η έννοια της ποιότητας των υπηρεσιών πρέπει να είναι σημαντική εντός του οργανισμού και να αποτελεί μέρος της νοοτροπίας κάθε εργαζομένου (Mateides & Dado, 2002).

Οι υπηρεσίες στις εγκαταστάσεις υγείας είναι άυλες και αφηρημένες. Ενώ στη βιομηχανία ο καθοριστικός παράγοντας είναι η ποιότητα του προϊόντος, στην υγειονομική περίθαλψη, η προσοχή εστιάζεται στις δραστηριότητες που λαμβάνουν χώρα στη σχέση μεταξύ ασθενών και επαγγελματιών υγείας. Ένα προϊόν κακής ποιότητας στον κλάδο σίγουρα δεν έχει τόσο μεγάλο αντίκτυπο στην ποιότητα της ζωής του πελάτη όσο μια κακή εξυπηρέτηση πελατών που παρέχεται στην υγειονομική περίθαλψη (Dernarova et al., 2008).

Οι δραστηριότητες ελέγχου αποτελούν το κύριο διαγνωστικό εργαλείο της ανώτατης διοίκησης και λειτουργούν ως αξιολόγηση και ανατροφοδότηση που παρέχει πληροφορίες για την κατάσταση του συστήματος ποιότητας των επιχειρήσεων, των οργανισμών και των διαδικασιών που λαμβάνουν χώρα σε αυτές. Οι έλεγχοι αποτελούν μια ανεξάρτητη πηγή πληροφοριών και καλύπτουν όλες τις διαδικασίες που συνθέτουν ένα σύστημα διασφάλισης ποιότητας.

Η διαδικασία ελέγχου θεωρείται σήμερα ως το μεγαλύτερο και πιο ευρέως χρησιμοποιούμενο εργαλείο διαχείρισης για τον προσδιορισμό του επιπέδου του συστήματος διαχείρισης ποιότητας. Οι εσωτερικοί έλεγχοι ποιότητας πραγματοποιούνται σε όλο τον οργανισμό και καλύπτουν όλους τους τομείς των παρεχόμενων υπηρεσιών. Για το σκοπό αυτό εκπαιδεύονται εσωτερικοί ελεγκτές ποιότητας. Το εύρος και το είδος της εκπαίδευσης καθορίζεται από έναν πάροχο υγειονομικής περίθαλψης. Τα αποτελέσματα του ελέγχου αναλύονται και χρησιμοποιούνται αποδεδειγμένα για τη βελτίωση της παρεχόμενης φροντίδας (Dernarova et al., 2008).

2.4. Η διαδικασία εσωτερικού ελέγχου στις υγειονομικές μονάδες

Ο εσωτερικός έλεγχος είναι μια ανεξάρτητη αξιολόγηση για την παροχή διαβεβαίωσης στον οργανισμό ότι οι οικονομικοί και λειτουργικοί έλεγχοι του είναι επαρκείς. Αυτή η διαδικασία συγκρίνει τις πολιτικές και τις διαδικασίες του οργανισμού σε σχέση με τις απαιτούμενες απαιτήσεις συμμόρφωσης. Οι ελεγκτές δεν είναι υπεύθυνοι για την εκτέλεση των δραστηριοτήτων του οργανισμού. Ωστόσο,

συμβουλεύουν τη διοίκηση και το διοικητικό συμβούλιο για το πώς να εκτελούν πιο αποτελεσματικά τις δραστηριότητές τους.

Με βάση την αξιολόγηση κινδύνου του οργανισμού, οι εσωτερικοί ελεγκτές, τα διοικητικά συμβούλια και τα συμβούλια εποπτείας καταρτίζουν και συμφωνούν για ένα ετήσιο σχέδιο ελέγχου. Συνήθως, αυτό το σχέδιο θα παρέχει μια σύντομη επισκόπηση των οντοτήτων που πρέπει να επανεξεταστούν και του χρονικού πλαισίου για τον έλεγχο που θα πραγματοποιηθεί. Πριν από την έναρξη του ελέγχου, η διοίκηση του οργανισμού αναπτύσσει και επανεξετάζει το εύρος και τους στόχους του ελέγχου.

Στη συνέχεια, ο εσωτερικός έλεγχος θα προχωρήσει σε επιτόπια εργασία, η οποία περιλαμβάνει συνεντεύξεις με την διοίκηση και δοκιμές, ανάλογα με το συγκεκριμένο εύρος του ελέγχου. Ο έλεγχος αξιολογεί τα μέσα που διαθέτει ο οργανισμός και, λαμβάνοντας υπόψη τους τρέχοντες κινδύνους και τις απαιτήσεις συμμόρφωσης, προσδιορίζει εάν χρειάζονται νέες διαδικασίες ή έλεγχοι. Μετά την ολοκλήρωση, προετοιμάζεται μια έκθεση με τα ευρήματα του ελέγχου και κοινοποιείται στον οργανισμό όπου αναπτύσσονται διορθωτικές ενέργειες από κοινού. Μετά από μια οριστική η έκθεση που συντάσσεται και εγκρίνεται από τη διοίκηση, παρουσιάζονται τα αποτελέσματα στην επιτροπή ελέγχου του οργανισμού.

Κάθε τομέας των εργασιών μπορεί να ελεγχθεί ως μέρος ενός εσωτερικού ελέγχου, συμπεριλαμβανομένων ορισμένων πτυχών που μπορεί να μην φαίνεται να εκτίθενται σε κίνδυνο. Οι στόχοι εσωτερικού ελέγχου που σχετίζονται με τους τομείς κινδύνου που περιγράφηκαν προηγουμένως περιλαμβάνουν (RSM, 2017):

- ✓ Διαδικασία Χρέωσης Ασθενών: Ο σκοπός αυτής της ανασκόπησης είναι να αξιολογήσει τις διαδικασίες και τους ελέγχους σχετικά με την ακρίβεια, την πληρότητα και την επικαιρότητα της σύλληψης, της καταγραφής και της συμφωνίας των χρεώσεων ασθενών. και για την αξιολόγηση των ελέγχων πρόσβασης στο σύστημα.
- ✓ Φαρμακείο: Ο σκοπός αυτής της ανασκόπησης είναι να αξιολογήσει τομείς όπως: αγορά και παραλαβή, διαχείριση συμβολαίων, έλεγχος αποθεμάτων, διανομή φαρμάκων, δέσμευση χρεώσεων, ελεγχόμενες ουσίες, ασφάλεια,

συμμόρφωση, αγορές συνταγών εργαζομένων, συστήματα πληροφοριών και λειτουργίες φαρμακείων εξωτερικών ασθενών.

- ✓ Μονοήμερη παραμονή: Ο σκοπός αυτής της ανασκόπησης είναι να αξιολογήσει την αποτελεσματικότητα των εσωτερικών ελέγχων καθώς σχετίζονται με την ιατρική λογική των εισαγωγών σε εσωτερικούς ασθενείς, καθώς και με την ικανότητα εντοπισμού εισαγωγών που δεν πληρούν τα κριτήρια εισαγωγής στο νοσηλευτικό ίδρυμα.
- ✓ Διαχείριση δραστηριοτήτων μετρητών: Ο σκοπός της επανεξέτασης είναι να προσδιορίσει εάν οι εσωτερικοί έλεγχοι είναι επαρκείς για τομείς που χειρίζονται άμεσα μετρητά. Αυτό περιλαμβάνει, αλλά δεν περιορίζεται σε, όλους τους χώρους των ταμείων που αφορούν τους ασθενείς, όλα τα ταμεία μικρομετρητών, τα ταμεία καφετέριας και τα μηχανήματα αυτόματης πώλησης.
- ✓ Εισαγωγή και εγγραφή ασθενών: Ο σκοπός αυτής της ανασκόπησης είναι: (1) να αξιολογήσει την επάρκεια του συστήματος εσωτερικού ελέγχου σε όλους τους χώρους εισαγωγής, συμπεριλαμβανομένου του τμήματος επειγόντων περιστατικών. (2) να προσδιορίσει εάν το σύστημα εσωτερικού ελέγχου λειτουργεί όπως προβλέπεται· (3) να καθορίσει ότι οι πόροι χρησιμοποιούνται με οικονομικό και αποδοτικό τρόπο. και (4) να διασφαλίζει ότι οι έλεγχοι σχετικά με τη σύλληψη, την καταγραφή και τη συλλογή εσόδων είναι επαρκείς.
- ✓ Εργαστήριο: Ο σκοπός αυτής της ανασκόπησης είναι να αξιολογήσει την επάρκεια του συστήματος εσωτερικών ελέγχων για το εργαστηριακό τμήμα, να καθορίσει εάν τα συστήματα ελέγχου λειτουργούν όπως προβλέπεται· και να διασφαλίσει τη συμμόρφωση με τις ισχύουσες πολιτικές και διαδικασίες.
- ✓ Φιλανθρωπική περίθαλψη: Ο σκοπός αυτής της ανασκόπησης είναι να αξιολογήσει την αποτελεσματικότητα των εσωτερικών ελέγχων που σχετίζονται με τις ακόλουθες οδηγίες που αφορούν στους οργανισμούς υγείας όσον αφορά τη φιλανθρωπική φροντίδα.

Υπάρχουν διάφορες στρατηγικές για την εκτέλεση ενός εσωτερικού ελέγχου. Η μεθοδολογία που παρουσιάζεται στην συνέχεια, είναι μια διαδικασία τεσσάρων βημάτων, λαμβάνοντας μια ολιστική ματιά στον οργανισμό και τις διαδικασίες του. Αυτά τα βήματα είναι η αξιολόγηση κινδύνου (όπως συζητήθηκε νωρίτερα), η

ανάπτυξη ετήσιου σχεδίου εσωτερικού ελέγχου, η ανάπτυξη και εκτέλεση προγράμματος ελέγχου και τα ευρήματα και οι συστάσεις.

Ανάπτυξη ετήσιου σχεδίου ελέγχου. Αφού πραγματοποιηθεί η αξιολόγηση κινδύνου, δημιουργείται ένα σχέδιο ελέγχου ανάλογα με τα ευρήματα και τις διαδικασίες του οργανισμού. Αυτό το σχέδιο προσδιορίζει τις βασικές διαδικασίες και τις ελεγχόμενες οντότητες που διαπιστώθηκε ότι απαιτούν τακτικές δοκιμές και εξετάσεις. Αυτές οι διεργασίες ταξινομούνται σύμφωνα με τον πιθανό κίνδυνο και τοποθετούνται σε εναλλαγή για να επιτραπεί η ευθυγράμμιση των διαθέσιμων πόρων και του χρονοδιαγράμματος ελέγχου.

Ανάπτυξη και εκτέλεση προγράμματος με βάση τον έλεγχο. Με βάση το σχέδιο ελέγχου που αναπτύχθηκε στο προηγούμενο βήμα, αναπτύσσονται σχέδια εργασίας για κάθε βασική διαδικασία και ελεγχόμενη οντότητα. Αναπτύσσεται ένα αρχικό σχέδιο ελέγχου, το οποίο αντιμετωπίζει τους στόχους κινδύνου και της διαδικασίας. Αυτό το σχέδιο περιλαμβάνει συνήθως μια λεπτομερή ανάλυση του στόχου του ελέγχου, του εύρους, της περιόδου, της ελεγχόμενης οντότητας, του ιδιοκτήτη της διαδικασίας, των βημάτων ελέγχου και της απαίτησης δοκιμής

Άλλα κοινά βήματα που λαμβάνουν χώρα στη διαδικασία ανάπτυξης και εκτέλεσης περιλαμβάνουν (RSM, 2017):

• Ανάπτυξη τεκμηρίωσης που περιγράφει λεπτομερώς τους διαδεδομένους κινδύνους, τις πιθανές επιπτώσεις τους και τις δραστηριότητες ελέγχου για τον μετριασμό τους

• Περιλήψεις δραστηριοτήτων ελέγχου για να διασφαλιστεί ότι αυτές εκτελούνται όπως περιγράφεται

• Σχεδιασμός σχεδίου δοκιμής, συμπεριλαμβανομένης της μεθοδολογίας δειγματοληψίας

• Ανάλυση εξαιρέσεων και παροχή βιώσιμων συστάσεων για τον μετριασμό της επανάληψης προβληματικών περιοχών

2.5 Αποτελέσματα εσωτερικών ελέγχων σε μονάδες υγείας στις ΗΠΑ

Από την άποψη της πληροφορικής, ο κλάδος της υγειονομικής περίθαλψης έχει εισέλθει σε μια νέα εποχή. Ποτέ δεν είχε δοθεί μεγαλύτερη έμφαση στην εφαρμογή και την εξάρτηση από μετασχηματιστικές νέες τεχνολογίες που προσφέρουν πολλά υποσχόμενα επιτεύγματα στη φροντίδα των ασθενών, τη λειτουργική αποτελεσματικότητα και την οργανωτική απόδοση. Η πρόσβαση σε ευαίσθητα δεδομένα υγειονομικής περίθαλψης γίνεται με πολλούς νέους τρόπους (Havens et al., 2020).

Αυτή η αλλαγή τροφοδοτεί την ιστορική καινοτομία. Ταυτόχρονα, εκθέτει τους οργανισμούς υγειονομικής περίθαλψης σε νέες προκλήσεις και κινδύνους. Το κυριότερο μεταξύ αυτών είναι η κυβερνο-ασφάλεια. Ενώ οι λειτουργίες εσωτερικού ελέγχου της υγειονομικής περίθαλψης πρέπει οπωσδήποτε να αντιμετωπίσουν ζητήματα κυβερνοασφάλειας, πρέπει να το πράξουν ενώ ασχολούνται με πολλές άλλες προτεραιότητες των οποίων ο αριθμός και η φύση συνεχίζουν να αλλάζουν λόγω του συνεχιζόμενου ψηφιακού μετασχηματισμού, των νέων ρυθμιστικών απαιτήσεων και της ασταθούς αγοράς.

Τα αποτελέσματα της Έρευνας Δυνατοτήτων και Αναγκών Εσωτερικού Ελέγχου των Οργανισμών Παρόχων Υγείας του 2020 από την AHIA και την Protiviti έριξαν φως στους τρόπους με τους οποίους τα διευθυντικά στελέχη του ελέγχου (CAE) και οι επαγγελματίες εσωτερικού ελέγχου εκτελούν αυτή τη στρατηγική παρέχοντας βεβαιότητα σε έναν συνεχώς αυξανόμενο αριθμό περιοχών κινδύνου. Τα αποτελέσματα υποδεικνύουν ότι οι πιο σημαντικές από αυτές τις ανταγωνιστικές προτεραιότητες περιλαμβάνουν τις ανταλλαγές πληροφοριών για την υγεία, τις ανταλλαγές ασφάλισης υγείας, το πλαίσιο του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) για τη βελτίωση της ασφάλειας στον κυβερνοχώρο και πολλαπλές πτυχές της πρόληψης απάτης (Havens et al., 2020).

Επιπλέον, τα αποτελέσματα δείχνουν ότι οι λειτουργίες εσωτερικού ελέγχου της υγειονομικής περίθαλψης εστιάζουν την προσοχή και τους πόρους τους σε πέντε βασικούς τομείς προτεραιότητας (Havens et al., 2020).:

1. Κίνδυνοι και πρακτικές κυβερνοασφάλειας

2. Κανονιστική συμμόρφωση

3. Υποστήριξη, ενεργοποίηση και προστασία της ψηφιακής επιχείρησης

4. Αντιμετώπιση κινδύνων απάτης

5. Συνεργασία πολλών μετόχων

Το μέγεθος, η συχνότητα και το κόστος των περιστατικών στον κυβερνοχώρο αυξάνονται δραματικά σε μια πληθώρα οικονομικών κλάδων. Οι οργανισμοί παροχής υγειονομικής περίθαλψης γνωρίζουν καλά αυτήν την ανησυχητική τάση, ιδιαίτερα δεδομένων των πρόσφατων κυβερνοεπιθέσεων που έχουν βιώσει πολλοί στον κλάδο τους τελευταίους μήνες. Το γεγονός είναι ότι οι απόπειρες παραβιάσεων φαίνονται σχεδόν σίγουρο ότι θα κλιμακωθούν για τους οργανισμούς παροχής υγειονομικής περίθαλψης, σε μεγάλο βαθμό λόγω της υψηλής αξίας που δίνουν οι εγκληματίες στα κλεμμένα δεδομένα υγειονομικής περίθαλψης.

Αυτοί οι κίνδυνοι επιδεινώνονται από τον αυξανόμενο αριθμό τρίτων προμηθευτών που έχουν πρόσβαση σε δεδομένα υγειονομικής περίθαλψης, καθώς τουλάχιστον μερικοί από τους οποίους ενδέχεται να έχουν κενά στην ασφάλεια των δεδομένων τους. Η διαχείριση κινδύνων από τον προμηθευτή παραμένει μια βασική ανησυχία. Επιπλέον, με πολλά νοσοκομεία και Υπεύθυνους Οργανισμούς Φροντίδας (ACO) να έχουν πρόσβαση στα ίδια συστήματα ηλεκτρονικών αρχείων υγείας (EHR) για δεδομένα και στατιστικές ασθενών, η πιθανότητα περιστατικών κυβερνοασφάλειας αυξάνεται (Havens et al., 2020).

Στη πιο πρόσφατη έρευνα, συμπεριέλαβαν οι ερευνητές μια ειδική ενότητα για την αξιολόγηση της τρέχουσας κατάστασης του κινδύνου για την ασφάλεια στον κυβερνοχώρο σε οργανισμούς παροχής υγειονομικής περίθαλψης. Τα αποτελέσματα υποδεικνύουν ότι οι λειτουργίες εσωτερικού ελέγχου θεωρούν ότι η ενίσχυση της ασφάλειας δεδομένων, η τήρηση του Πλαισίου των Προτύπων του Εθνικού Ινστιτούτου Τεχνολογίας (NIST) «Framework for Improving Critical Infrastructure Cybersecurity» και οι δυνατότητες της νέας ανάλυσης δεδομένων και τεχνολογίας ελέγχου είναι μεταξύ των υψηλότερων προτεραιοτήτων τους (Havens et al., 2020).

Συγκεκριμένα, τα αποτελέσματά δείχνουν τα εξής (Association of Healthcare Internal Auditors, 2015):

• Γενικά λείπει η εμπιστοσύνη μεταξύ των ηγετών εσωτερικού ελέγχου και των επαγγελματιών σχετικά με τις τρέχουσες δυνατότητες κυβερνοασφάλειας των οργανισμών παροχής υγειονομικής περίθαλψης, συμπεριλαμβανομένου του εντοπισμού, της αξιολόγησης και του μετριασμού του κινδύνου για την ασφάλεια στον κυβερνοχώρο σε αποδεκτό επίπεδο.

• Το επίπεδο ευαισθητοποίησης των ανώτερων στελεχών σχετικά με τις εκθέσεις ασφάλειας πληροφοριών είναι ένας τομέας προς βελτίωση.

• Κατά μέσο όρο, ένας στους τρεις οργανισμούς παροχής υγειονομικής περίθαλψης στερείται στρατηγικής κινδύνου στον κυβερνοχώρο καθώς και πολιτικής κινδύνου στον κυβερνοχώρο.

• Από τη θετική πλευρά, η μεγάλη πλειονότητα των οργανισμών παροχής υγειονομικής περίθαλψης περιλαμβάνουν τον κίνδυνο κυβερνοασφάλειας στην αξιολόγηση κινδύνου.

Στην συνέχεια, παρουσιάζονται δέκα στοιχεία δράσης για την κυβερνοασφάλεια για τους οργανισμούς Υγείας και τον εσωτερικό έλεγχο (Association of Healthcare Internal Auditors, 2015).

1. Συνεργασία με τη διοίκηση και το διοικητικό συμβούλιο για την ανάπτυξη στρατηγικής και πολιτικής για την ασφάλεια στον κυβερνοχώρο.

2. Επιδίωξη για να επιτύχει ο οργανισμός υψηλό επίπεδο αποτελεσματικότητας στην ικανότητά του να εντοπίζει, να αξιολογεί και να μετριάζει τον κίνδυνο κυβερνοασφάλειας σε αποδεκτό επίπεδο.

3. Αναγνώριση της απειλής παραβίασης της κυβερνοασφάλειας που προκύπτει από τις ενέργειες ενός υπαλλήλου ή ενός επιχειρηματικού εταίρου.

4. Μόχλευση των σχέσεων του διοικητικού συμβουλίου για (α) ενίσχυση της ευαισθητοποίησης και της γνώσης του συμβουλίου σχετικά με τον κίνδυνο της κυβερνοασφάλειας. και (β) για να διασφαλιστεί ότι το διοικητικό συμβούλιο

παραμένει ιδιαίτερα αφοσιωμένο σε θέματα κυβερνοασφάλειας και ενημερωμένο σχετικά με τη μεταβαλλόμενη φύση και τη στρατηγική σημασία του κινδύνου για την ασφάλεια στον κυβερνοχώρο.

5. Διαβεβαίωση ότι ο κίνδυνος κυβερνοασφάλειας είναι επίσημα ενσωματωμένος στο σχέδιο ελέγχου.

6. Ανάπτυξη και διατήρηση της ενημερωμένης κατανόησης του πώς οι αναδυόμενες τεχνολογίες και οι τεχνολογικές τάσεις επηρεάζουν την εταιρεία και το προφίλ κινδύνου στον κυβερνοχώρο.

7. Αξιολόγηση του προγράμματος κυβερνοασφάλειας του οργανισμού σε σχέση με το Πλαίσιο Κυβερνοασφάλειας NIST, αναγνωρίζοντας παράλληλα ότι το πλαίσιο δεν πηγαίνει σε επίπεδο ελέγχου και επομένως ενδέχεται να απαιτούνται πρόσθετες αξιολογήσεις των προτύπων ISO 27001 και 27002.

8. Αναγνώριση του ότι, όσον αφορά την ασφάλεια στον κυβερνοχώρο, η ισχυρότερη προληπτική ικανότητα απαιτεί συνδυασμό ανθρώπινης και τεχνολογικής ασφάλειας, δηλαδή έναν συμπληρωματικό συνδυασμό εργαλείων εκπαίδευσης, ευαισθητοποίησης, επαγρύπνησης και τεχνολογίας.

9. Ενίσχυση της ανάγκης παρακολούθησης της κυβερνοασφάλειας και αντιμετώπισης συμβάντων στον κυβερνοχώρο με τη διαχείριση, μέσα από την ύπαρξη ενός σαφούς πρωτόκολλου κλιμάκωσης μπορεί να βοηθήσει στην υποστήριξη (και στη διατήρηση) αυτής της προτεραιότητας.

10. Επισήμανση τυχόν ελλείψεων προσωπικού πληροφορικής, ελεγκτών και πόρων, οι οποίες αντιπροσωπεύουν κορυφαία τεχνολογική πρόκληση σε πολλούς οργανισμούς και μπορούν να παρεμποδίσουν τις προσπάθειες αντιμετώπισης ζητημάτων ασφάλειας στον κυβερνοχώρο.

Επιπλέον, όταν πρόκειται για την αξιολόγηση της ισχύος των τρεχόντων μέτρων κυβερνοασφάλειας, το Πλαίσιο Κυβερνοασφάλειας NIST μπορεί να χρησιμεύσει ως χρήσιμη λυδία λίθος για οργανισμούς και λειτουργίες εσωτερικού ελέγχου. Πολλές ιδιότητες αυτού του πλαισίου περιγράφουν επίσης βασικές πτυχές των ηγετικών πρακτικών στον εσωτερικό έλεγχο, καθώς βασίζεται στον κίνδυνο,

είναι συμπληρωματικό με άλλα προγράμματα κινδύνου και υπόκειται σε αλλαγές και βελτιώσεις. Ωστόσο, από τεχνική άποψη, η συμμόρφωση με το NIST είναι εθελοντική με την κανονιστική έννοια (όμως απαιτείται από άποψη διακυβέρνησης).

Περισσότερες λειτουργίες εσωτερικού ελέγχου ανακαλύπτουν ότι η προσέγγιση του πλαισίου NIST αντικατοπτρίζει τις υπάρχουσες αξιολογήσεις προγραμμάτων τους (Association of Healthcare Internal Auditors, 2015):

1. Καθορισμός των επιχειρηματικών προτεραιοτήτων και του πεδίου εφαρμογής του προγράμματος (κυβερνοασφάλεια).

2. Προσδιορισμός των περιουσιακών στοιχείων σε εύρος και τις απειλές για αυτά.

3. Δημιουργία ενός προφίλ "default" ή βασικού προφίλ για την υλοποίηση του προγράμματος ασφάλειας του οργανισμού.

4. Πραγματοποίηση αξιολόγησης κινδύνου για την ετοιμότητα του οργανισμού.

5. Δημιουργία μιας δήλωσης- στόχο για το πρόγραμμα ασφαλείας.

6. Καθορισμός των κενών μεταξύ των καταστάσεων «Όπως είναι στην πραγματικότητα» και «όπως θα έπρεπε να είναι», αξιολόγηση του αντίκτυπού τους και έμφαση προτεραιότητα στις δραστηριότητες αποκατάστασης.

Όσον αφορά το τελευταίο σημείο, αυτά τα κενά είναι φυσικά κρίσιμα. Οι εσωτερικοί ελεγκτές γίνονται μάρτυρες αυτού του είδους κενού όταν συνειδητοποιούν ότι το πλαίσιο NIST είναι ατελές, καθώς δεν φτάνει στο επίπεδο ελέγχου, όπου μπορούν να εφαρμοστούν τα πρότυπα ISO 27000 (ασφάλεια πληροφοριών). Οι έμπειροι εσωτερικοί ελεγκτές είναι ικανοί να καλύψουν ένα ευρύ φάσμα κενών διαχείρισης κινδύνου και γνώσεων. Αυτό εξηγεί γιατί το ISO 27000 (ασφάλεια πληροφοριών) συγκαταλέγεται στις 10 κορυφαίες προτεραιότητες για τους εσωτερικούς ελεγκτές τα τελευταία χρόνια.

2.6 Αποτελέσματα εσωτερικών ελέγχων σε μονάδες υγείας στην Ελλάδα

Η δημόσια υγεία είναι η επιστήμη της πρόληψης ασθενειών και της παράτασης της ζωής. Επηρεάζει τις ζωές των ανθρώπων καθημερινά και σε κάθε μέρος του κόσμου. Είναι λοιπόν στην πολιτική ατζέντα κάθε σύγχρονης κοινωνίας και θα είναι για τις επόμενες γενιές. Στην ΕΕ, η δημόσια υγεία είναι κυρίως ευθύνη των κρατών μελών της ΕΕ. Ως εκ τούτου, τα συστήματα υγείας διαφέρουν σημαντικά μεταξύ των κρατών μελών της ΕΕ. Η Ευρωπαϊκή Ένωση υποστηρίζει τις προσπάθειες σε εθνικό επίπεδο, με ιδιαίτερη έμφαση στη συμπλήρωση ή στο συντονισμό των δράσεων των κρατών μελών στον τομέα της δημόσιας υγείας. Κατά συνέπεια, η δημόσια υγεία, ιδωμένη από την οπτική γωνία της ΕΕ, είναι ένας πολύπλοκος τομέας για έλεγχο. Ωστόσο, λόγω της σημασίας της δημόσιας υγείας, τα Ανώτατα Ελεγκτικά Όργανα της ΕΕ έχουν πραγματοποιήσει πολλούς ελέγχους σε συναφή θέματα.

Το ελληνικό ΣτΕ αξιολόγησε τη συσσώρευση ληξιπρόθεσμων οφειλών του Δημοσίου. Ο έλεγχος κάλυψε την περίοδο από 31 Δεκεμβρίου 2016 έως 30 Σεπτεμβρίου 2017. Τα κύρια ερωτήματα του ελέγχου ήταν (Contact Committee of the Supreme Audit Institutions of the European Union, 2019):

- ✓ Έχει χρησιμοποιηθεί η χρηματοδότηση του Ευρωπαϊκού Μηχανισμού Σταθερότητας για την εκκαθάριση ληξιπρόθεσμων οφειλών για τον επιδιωκόμενο σκοπό;
- ✓ Γιατί συνεχίζουν να συσσωρεύονται ληξιπρόθεσμες οφειλές;

Οι κύριοι ελεγχόμενοι ήταν έξι νοσοκομεία, ο Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας (ΕΟΠΥΥ) και η Α’ Διεύθυνση Υγείας Περιφέρειας Αττικής. Τα στοιχεία ελήφθησαν κυρίως από συνεντεύξεις, επιστολές εκκαθάρισης σε τρίτους (προμηθευτές), αιφνιδιαστικούς επιτόπιους ελέγχους παραδόσεων αγαθών και υπηρεσιών, ελέγχους εγγράφων και επαλήθευση της νομιμότητας και κανονικότητας εγγράφων και διαδικασιών.

Ο έλεγχος αποκάλυψε (Contact Committee of the Supreme Audit Institutions of the European Union, 2019):

- ✓ παρατυπίες στη ωρίμανση των ληξιπρόθεσμων οφειλών και ελλιπή δικαιολογητικά ή έγγραφα πληρωμής σχετικά με προμήθειες και υπηρεσίες·
- ✓ έλλειψη μηχανισμών παρακολούθησης της πληρωμής τόκων και οικονομικών κυρώσεων και μητρώων σχετικά με την κατάσταση των δικαστικών υποθέσεων·
- ✓ ότι σημαντικός αριθμός υποχρεώσεων δεν είχε εγγραφεί ή είχε καταχωρηθεί εσφαλμένα στο Μητρώο Δεσμεύσεων ή δεν είχε καταχωρηθεί στα συστήματα πληροφορικής·
- ✓ ότι τα συστήματα πληροφορικής απέτυχαν να εξάγουν συγκεκριμένες συγκεντρωτικές και αναλυτικές αναφορές σχετικά με την αντιστάθμιση.

Ως προς το πρόγραμμα εκκαθάρισης ληξιπρόθεσμων οφειλών, το ελληνικό ΣτΕ βρήκε περιπτώσεις μη συμμόρφωσης με τον κανόνα FIFO και με τα χρονικά όρια για την εκκαθάριση των υποχρεώσεων, αποκλίσεις μεταξύ των ελεγμένων εγγράφων και ελλείψεις στη διαδικασία πληρωμής. Τα ευρήματα σχετικά με την αξιοπιστία των δεδομένων και των συστημάτων αναφοράς αφορούσαν κυρίως τα συστήματα καταγραφής υποχρεώσεων και επιπλέον έχουν εντοπιστεί αποκλίσεις μεταξύ των συστημάτων αναφοράς.

Ο έλεγχος επικεντρώθηκε περαιτέρω στον εντοπισμό πηγών νέων ληξιπρόθεσμων οφειλών. Τα ευρήματα ήταν τα εξής (Contact Committee of the Supreme Audit Institutions of the European Union, 2019):

- ✓ Έλλειψη ρευστότητας που οφείλεται σε μη ρεαλιστικούς προϋπολογισμούς,
- ✓ επιβολή ανώτατων ορίων δαπανών από τον Ευρωπαϊκό Μηχανισμό Σταθερότητας,
- ✓ καθυστερήσεις στην εφαρμογή μηχανισμών εκπτώσεων και ανάκτησης,
- ✓ καθυστερήσεις στην είσπραξη εσόδων και
- ✓ μείωση των σχετικών απαιτήσεων βάσει ειδικών ρυθμίσεων.

Λόγω της πολυπλοκότητας (και σε ορισμένες περιπτώσεις ασάφειας) του νομοθετικού πλαισίου που διέπει τις διαδικασίες σύναψης συμβάσεων, οι διαδικασίες διαγωνισμών δεν ολοκληρώνονταν πάντα (ως αποτέλεσμα της γραφειοκρατίας και του περιορισμού του νομοθετικού πλαισίου που οδηγεί σε αμέτρητες δεσμεύσεις και

καθυστερήσεις στις αποπληρωμές λόγω ζητήματα νομιμότητας), και απαιτήθηκε μεγάλος όγκος δικαιολογητικών για την εκκαθάριση των ληξιπρόθεσμων οφειλών.

Η αξιολόγηση των αποτελεσμάτων του προγράμματος πληρωμών ληξιπρόθεσμων οφειλών αποκάλυψε ότι το πρόγραμμα δεν ήταν αρκετά ώριμο και ότι, σε ορισμένες περιπτώσεις, δεν είχε τηρηθεί ο κανόνας της αυτοχρηματοδότησης –δηλαδή η πληρωμή των ιδίων υποχρεώσεων των οντοτήτων με δικούς τους πόρους. .

Το ελληνικό ΣτΕ συνιστά (Contact Committee of the Supreme Audit Institutions of the European Union, 2019):

- ✓ την αναβάθμιση των συστημάτων πληροφορικής και την υποστήριξή τους για τακτικούς προϋπολογισμούς·
- ✓ Χρησιμοποίηση αυτών των συστημάτων για να εξαχθούν αυτόματα όλες οι απαιτούμενες αναφορές.
- ✓ Ενημέρωση αυτόματα το Μητρώου Δεσμεύσεων, ώστε αυτό να είναι σε θέση να προβεί σε συγκεκριμένες αλλαγές και βελτιώσεις σε αυτό, προκειμένου να διασφαλιστεί η νομιμότητα και κανονικότητα της καταγραφής και πληρωμής των υποχρεώσεων και των ληξιπρόθεσμων οφειλών·
- ✓ Εφαρμογή της μέθοδο "First-In-First-Out" κατά την πληρωμή των υποχρεώσεων και ο αυτόματος συμψηφισμός των πληρωμών με παλαιότερα τιμολόγια.
- ✓ να καταστηθεί πλήρως λειτουργικός ο εθνικός κεντρικός φορέας αγορών για τον τομέα της δημόσιας υγείας·
- ✓ καθιέρωση πρωτοκόλλων παραγωγής με ιατρική διαδικασία,
- ✓ εσωτερικούς ελέγχους στις διοικητικές διαδικασίες προμήθειας και πληρωμής,
- ✓ ενιαία κωδικοποίηση και ταξινόμηση,
- ✓ ενιαίες Τεχνικές Προδιαγραφές,
- ✓ κοινούς γραμμωτούς κώδικες και μητρώα για αναλώσιμα, υλικά και ιατρικό εξοπλισμό.
- ✓ βελτίωση της διαχείρισης των αποθεμάτων·
- ✓ επιτάχυνση της αξιολόγησης των προσφορών στις διαδικασίες ανάθεσης συμβάσεων·
- ✓ εδραίωση και υιοθέτηση κοινού συστήματος πληροφορικής σε όλα τα νοσοκομεία·

- ✓ Εφαρμογή δεικτών KPI,
- ✓ δεικτών αναφοράς,
- ✓ λογιστικής κόστους και
- ✓ και συστήματος λογιστικής που βασίζεται σε δεδουλευμένη βάση·
- ✓ να εφαρμοστεί εγκαίρως, ο μηχανισμός επιστροφής χρημάτων clawback στους παρόχους περίθαλψης·
- ✓ Ανάπτυξη ρεαλιστικών προϋπολογισμών·
- ✓ θέσπιση εσωτερικών κανόνων,
- ✓ εσωτερικοί έλεγχοι ανά διαδικασία και
- ✓ εγχειρίδιο εσωτερικού ελέγχου·
- ✓ βελτίωση της διαδικασίας ανάλυσης κινδύνου στα νοσοκομεία·
- ✓ βελτίωση της επάρκειας και της κατανομής του προσωπικού·
- ✓ επιτάχυνση των διαδικασιών εκκαθάρισης και πληρωμής· και
- ✓ πληρωμή των κρατικών επιδοτήσεων σε μηνιαία βάση.

3. Η σημασία της προστασίας των προσωπικών δεδομένων στον χώρο της υγείας και ο ρόλος του εσωτερικού έλεγχου

3.1 Ο ρόλος της πληροφορικής στην προστασία των προσωπικών δεδομένων των ασθενών

Ενώ η ασφάλεια ΤΠ αφορούσε παραδοσιακά την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, η προστασία δεδομένων συνδέθηκε με το απόρρητο της επεξεργασίας. Τα τελευταία χρόνια, αυτά τα θέματα συγχωνεύονται όλο και περισσότερο και ρυθμιστικές πράξεις όπως ο GDPR ορίζουν πολύ αυστηρές απαιτήσεις ασφάλειας δεδομένων για τους υπεύθυνους επεξεργασίας δεδομένων (European Union Agency for Cybersecurity, 2018).

Αυτό σημαίνει ότι οι υπεύθυνοι επεξεργασίας (και οι εκτελούντες την επεξεργασία) πρέπει να διαθέτουν τα κατάλληλα μέτρα ασφαλείας για να αποτρέψουν την τυχαία ή εσκεμμένη παραβίαση των προσωπικών δεδομένων που διατηρούν. Ως εκ τούτου, οι ελεγκτές θα πρέπει να έχουν κατά νου ότι ενώ η ασφάλεια των πληροφοριών περιορίζεται μερικές φορές στην ασφάλεια στον κυβερνοχώρο (η προστασία των δικτύων και των συστημάτων πληροφοριών από επιθέσεις), καλύπτει επίσης άλλα πράγματα όπως φυσικά και οργανωτικά μέτρα ασφάλειας.

Έτσι, τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την προστασία των προσωπικών δεδομένων είναι ζωτικής σημασίας για τη διατήρηση της εμπιστοσύνης των υποκειμένων των δεδομένων στην επεξεργασία και θα βοηθήσουν τα συστήματα δημόσιας υγείας να εξασφαλίσουν τη δημόσια υποστήριξη και τη συμμόρφωση των υποκειμένων των δεδομένων. Τα μέτρα μπορεί να περιλαμβάνουν όχι μόνο τεχνικά μέτρα –όπως κρυπτογράφηση δεδομένων, αλλά και σταθερές προσεγγίσεις διαχείρισης ταυτότητας και πρόσβασης ή διαχείρισης δεδομένων, συμπεριλαμβανομένης της ταξινόμησης δεδομένων (για παράδειγμα, ως αυστηρά εμπιστευτικά/εμπιστευτικά/δημόσια). Μια βασική πτυχή της προστασίας είναι η αυστηρή διαχείριση των δικαιωμάτων διαχείρισης και πρόσβασης. Τα δημόσια

ιδρύματα υγείας –και τα ιδρύματα υγείας γενικά– συχνά αποτυγχάνουν να εφαρμόσουν μια αυστηρή αρχή της «ανάγκης γνώσης» (European Union Agency for Cybersecurity, 2018).

Κανονισμοί όπως ο GDPR ενδέχεται να μην περιγράφουν τα ακριβή μέτρα ασφαλείας που απαιτούνται. Αντίθετα, απαιτούν από τους ελεγκτές να έχουν ένα επίπεδο ασφάλειας που είναι «κατάλληλο» για τους κινδύνους που παρουσιάζει η επεξεργασία. Οι αρχές δημόσιας υγείας και άλλοι παράγοντες του τομέα πρέπει να το λάβουν υπόψη σε σχέση με τις τελευταίες εξελίξεις και το κόστος εφαρμογής, καθώς και με τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τον σκοπό της επεξεργασίας.

Έχοντας υπόψη ότι ο τομέας της δημόσιας υγείας είναι συχνά επιφορτισμένος με την επεξεργασία ευαίσθητων προσωπικών δεδομένων, όπως δεδομένα που σχετίζονται με την υγεία και τη σωματική ευεξία, τα υποκείμενα των δεδομένων θα αναμένουν πολύ υψηλό επίπεδο ασφάλειας δεδομένων σε τέτοιες λειτουργίες. Τούτου λεχθέντος, η μη διαθεσιμότητα κεφαλαίων για μέτρα ασφαλείας δεδομένων δεν αποτελεί δικαιολογία, στο βαθμό που τα μέτρα αυτά είναι απαραίτητα για την επίτευξη ενός «κατάλληλου» επιπέδου προστασίας.

Ένα σημαντικό θέμα είναι ο χειρισμός παραβιάσεων δεδομένων – παραβιάσεις της ασφάλειας που οδηγούν σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα. Αυτό περιλαμβάνει παραβιάσεις που είναι αποτέλεσμα τυχαίας και εσκεμμένης ενέργειας . Τα ιδρύματα οποιουδήποτε μεγέθους ή εγκατάστασης κατακλύζονται εύκολα από μια κατάσταση παραβίασης δεδομένων. Ως εκ τούτου, συνιστάται στα δημόσια ιδρύματα υγείας να προγραμματίσουν αυτό το ενδεχόμενο, ενδεχομένως ακόμη και με τη διεξαγωγή μιας προσομοίωσης κάποιου περιστατικού στον κυβερνοχώρο. Απαιτείται ένα σχέδιο παραβίασης δεδομένων – με σαφή κατανομή καθηκόντων και ευθυνών –, συμπεριλαμβανομένης μιας στρατηγικής επικοινωνίας για παραβίαση δεδομένων (Wilmslom, 2020).

Ένα σημαντικό εργαλείο είναι οι τακτικές δοκιμές διείσδυσης, που πραγματοποιούνται από ανεξάρτητο τρίτο μέρος: με απλά λόγια, ένας υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να προσκαλεί «ηθικούς χάκερ» να δοκιμάσουν τις αδυναμίες του συστήματος. Πολλές χώρες διαθέτουν υπηρεσίες ασφάλειας

πληροφορικής ή κυβερνοασφάλειας που υποστηρίζουν τα δημόσια ιδρύματα υγείας στη δημιουργία τέτοιων ιδεών. Για ιδρύματα που εξυπηρετούν λειτουργικούς σκοπούς, ένα σχέδιο αποκατάστασης από καταστροφές είναι εξίσου κρίσιμο και αυστηρά απαραίτητο

Έτσι, τα συστήματα λογισμικού που ασχολούνται με ευαίσθητα και προσωπικά δεδομένα χρηστών αντιμετωπίζουν κρίσιμα εμπόδια σχετικά με το ζήτημα της διατήρησης υψηλού επιπέδου αποτελεσματικού απορρήτου δεδομένων τα τελευταία χρόνια. Σε οποιοδήποτε σύστημα πληροφοριών, το απόρρητο και η εμπιστευτικότητα είναι οι βασικοί στόχοι ασφάλειας που πρέπει να λαμβάνονται υπόψη. Οι περισσότερες ηλεκτρονικές υπηρεσίες εξαρτώνται από αποθηκευμένα δεδομένα για την αναγνώριση των προσωπικών και ιατρικών αρχείων ενός χρήστη. Παρά τη σημασία του, το ζήτημα του απορρήτου θεωρείται συχνά ως εκ των υστέρων σκέψη, κυρίως λόγω της ανεπαρκούς τεχνογνωσίας και της σχετικής ευαισθητοποίησης μεταξύ των σχεδιαστών και των προγραμματιστών συστημάτων. Οι απαιτήσεις ασφαλείας ενδέχεται να παρακάμψουν τους θεμελιώδεις στόχους της ιδιωτικής ζωής, εάν οι απαιτήσεις απορρήτου δεν εφαρμόζονται με αρκετή σαφήνεια (Kalloniatis et al., 2008).

Οι σύγχρονες προκλήσεις της προστασίας δεδομένων και της εφαρμογής των σωστών ρυθμιστικών προτύπων για τα περιουσιακά στοιχεία του οργανισμού έναντι της αυξανόμενης απειλής των απειλών στον κυβερνοχώρο αποτελούν μεγάλη ανησυχία για τους οργανισμούς σε όλο τον κόσμο. Η έκθεση του Υπουργείου Υγείας και Ανθρωπίνων Υπηρεσιών (HHS) των ΗΠΑ για το 2018 αναφέρει ότι 6,1 εκατομμύρια άτομα επηρεάζονται από 229 παραβιάσεις δεδομένων υγειονομικής περίθαλψης και αυτές οι πληροφορίες αναφέρθηκαν στην πύλη παραβίασης των πολιτικών δικαιωμάτων (Weisbaum, 2018).

Η Statista αναφέρει ότι ο αριθμός των παραβιάσεων δεδομένων στις ΗΠΑ βρίσκεται σε ανοδική τάση από το 2005. Συνολικά αναφέρθηκαν 783 παραβιάσεις δεδομένων το 2014, με περίπου 85,61 εκατομμύρια συνολικές εγγραφές να έχουν παραβιαστεί, που ήταν μια αύξηση περίπου 500% από το 2005. Αυτός ο αριθμός αυξήθηκε υπερδιπλασιασμένος σε 1579 σε 3 χρόνια, όπως αναφέρθηκε για το 2017. Ομοίως, από την 1η Απριλίου έως τις 30 Ιουνίου 2018, οι πάροχοι υπηρεσιών υγειονομικής περίθαλψης υπέστησαν τον μεγαλύτερο αριθμό παραβιάσεων

δεδομένων από οποιονδήποτε άλλο τομέα στην Αυστραλία, όπου 49 από τις 242 παραβιάσεις αναφέρθηκαν από τους τομείς της υγειονομικής περίθαλψης λόγω ανθρώπινων σφαλμάτων σύμφωνα με το Office of the Australian Information Commissioner (Digital Guardian, 2018).

Η μέση οικονομική απώλεια μιας παραβίασης που περιλαμβάνει 1 εκατομμύριο εγγραφές είναι σχεδόν 40 εκατομμύρια AUD. Επί του παρόντος, οι τομείς υγειονομικής περίθαλψης στην Αυστραλία αλλά και σε άλλες χώρες, έχουν αυτοματοποιηθεί και έτσι, τα προσωπικά αρχεία, τα κλινικά δεδομένα, η αποθήκευση και άλλες σχετικές πληροφορίες των ασθενών αποθηκεύονται μέσω κάποιου ηλεκτρονικού μέσου. Οι ασθενείς, οι ιατροί και οι πάροχοι ιατρικών υπηρεσιών συνεργάζονται με πιο ευαίσθητες πληροφορίες από ποτέ. Πρόσφατες σημαντικές απειλές για το απόρρητο δεδομένων προέκυψαν λόγω μη εξουσιοδοτημένης πρόσβασης, κλοπής δεδομένων, απώλειας δεδομένων και ακατάλληλης διάθεσης δεδομένων και περιστατικών παραβίασης IT (Weisbaum, 2018).

Οι οργανισμοί υγειονομικής περίθαλψης είχαν το υψηλότερο κόστος που σχετίζεται με μεμονωμένη παραβίαση δεδομένων, το οποίο είναι τρεις φορές υψηλότερο από το μέσο όρο. Πολλοί από αυτούς έχουν αρχίσει να υιοθετούν διάφορες λύσεις που βασίζονται στο Blockchain για την εφαρμογή ασφαλών αποκεντρωμένων αρχείων ασθενών που βασίζονται σε Blockchain και την παρακολούθηση της προόδου των ασθενών, τόσο από απόσταση όσο και επιτόπου, με πλήρη προστασία δεδομένων έναντι διαρροής σε τρίτους (Weisbaum, 2018).

Το Privacy by design (PbD) είναι μια διαδικασία που βασίζεται στην προληπτική ενσωμάτωση καλών πρακτικών απορρήτου στο σχεδιασμό και τη λειτουργία συστημάτων πληροφορικής, φυσικής υποδομής και επιχειρηματικών πρακτικών. Το PbD στοχεύει στη διασφάλιση της ιδιωτικής ζωής και στην απόκτηση προσωπικού ελέγχου στις πληροφορίες των ατόμων, με αποτέλεσμα ένα βιώσιμο ανταγωνιστικό πλεονέκτημα για τους οργανισμούς. Ο κίνδυνος παραβίασης δεδομένων αυξάνεται κάθε χρόνο, με πολλούς οργανισμούς να πέφτουν θύματα παραβιάσεων δεδομένων σε όλο τον κόσμο, που μέχρι στιγμής έχουν αγωνιστεί να βρουν αποτελεσματικές λύσεις. Σήμερα, το να κάνει κάποιος μηχανισμός εξασφάλισης τον χρήστη να εμπιστευτεί το σύστημα για την εκτέλεση καθημερινών

δραστηριοτήτων για τις προσωπικές ή επαγγελματικές του ανάγκες είναι μια μεγάλη πρόκληση στον τομέα της μηχανικής λογισμικού (Whigham, 2020).

Για να διευθετηθεί αυτή η ανησυχία, εμπειρογνώμονες που εργάζονται με μηχανισμούς προστασίας δεδομένων έχουν υποστηρίξει την πρακτική της προστασίας της ιδιωτικής ζωής μέσω στρατηγικών σχεδιασμού τέτοιων που λαμβάνουν υπόψη τις απαιτήσεις απορρήτου που ξεκινούν απευθείας από την ίδρυση της φάσης του σχεδιασμού. Το απόρρητο προσδιορίζεται από την έννοια του PbD ως ένα κριτήριο σχεδιασμού που απαιτείται καθώς λαμβάνεται υπόψη κατά το στάδιο σχεδιασμού του συστήματος (Whigham, 2020).

Οι Geoff et al. (2007) ανέφεραν ότι είναι απαραίτητο να οικοδομηθεί ένα κοινό πλαίσιο στο οποίο οι προσεγγίσεις μπορούν να αναλυθούν βάζοντας τις προηγούμενες προσεγγίσεις σε μια προοπτική. Ο σχεδιασμός ενός συστήματος ευαίσθητου στην προστασία της ιδιωτικής ζωής πρέπει να λαμβάνει υπόψη τον παρατηρητή και το παρατηρούμενο, καθώς και τη σύνδεση μεταξύ τους. Αυτό το πλαίσιο έχει σχεδιαστεί για την εφαρμογή μέτρων απορρήτου στα πανταχού παρόντα υπολογιστικά περιβάλλοντα και έχει αποδείξει την εφαρμογή του σε όλη την υγειονομική περίθαλψη. Το κενό σε αυτό το πλαίσιο είναι η ευαισθησία του περιβάλλοντος υγειονομικής περίθαλψης και των σχετικών δεδομένων του, τα οποία θα παίξουν μεγάλο ρόλο στις αιτήσεις υιοθέτησης για διάχυτη υγειονομική περίθαλψη.

Ο Kenthapadi (2006) έχει ερευνήσει το θέμα του «Μοντέλου ελέγχου ερωτημάτων για το απόρρητο δεδομένων». Σε αυτό το πλαίσιο, χρησιμοποιείται ένας μηχανισμός απορρήτου για την υποβολή ερωτημάτων στη βάση δεδομένων που απορρίπτει το ερώτημα και αλλάζει την απάντηση προκειμένου να διασφαλιστεί το απόρρητο. Ένα σημαντικό ζήτημα αυτής της έρευνας είναι ότι η άρνηση ερωτήματος μπορεί να διαρρεύσει πληροφορίες, και έτσι ένας εισβολέας μπορεί να χρησιμοποιήσει προηγουμένως προτεινόμενους ελεγκτές για να θέσει σε κίνδυνο το απόρρητο ενός μεγάλου μέρους προσωπικών δεδομένων.

3.2. Νομικά και θεσμικά μέσα προστασίας των προσωπικών δεδομένων των ασθενών

Τις τελευταίες τρεις δεκαετίες, το επίπεδο ρύθμισης στον τομέα της προστασίας δεδομένων και της ασφάλειας στον κυβερνοχώρο έχει αυξηθεί. Στην παράγραφο αυτή, δίνεται λιγότερη έμφαση σε έγγραφα υψηλού επιπέδου, όπως ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ και, περισσότερο, εξετάζεται το επίπεδο ρύθμισης που είναι πιο κοντά στους επαγγελματίες που δραστηριοποιούνται στον τομέα της Υγείας.

Για να γίνει αυτό, είναι σημαντικό να γίνει διάκριση μεταξύ ειδικών τομεακών νόμων που ρυθμίζουν την επεξεργασία δεδομένων υγείας, γενικών νόμων προστασίας δεδομένων (όπως ο GDPR) και νόμων που διέπουν την επεξεργασία προσωπικών δεδομένων και μπορεί να έχουν άμεσες ή έμμεσες συνέπειες στα συστήματα Υγείας (όπως π.χ. ως ePrivacy) (WHO, 2020).

Οι ειδικοί τομεακοί νόμοι είναι σημαντικοί στο βαθμό που παρέχουν σαφείς οδηγίες για την επεξεργασία προσωπικών δεδομένων για σκοπούς υγείας και συχνά χρησιμεύουν ως νομική βάση για δραστηριότητες επεξεργασίας. Τέτοιοι νόμοι μπορεί είτε να αφορούν συγκεκριμένα καθήκοντα δημόσιας υγείας (όπως ένα μητρώο καρκίνου) είτε να διέπουν τη χρήση των πληροφοριών υγείας σε κλινικό/ιατρικό περιβάλλον (όπως συμβαίνει με τα ηλεκτρονικά αρχεία υγείας), με επακόλουθη δευτερογενή χρήση δεδομένων για σκοπούς δημόσιας υγείας. Στην πραγματικότητα, η προστασία δεδομένων απαιτεί την ανάπτυξη και εφαρμογή τέτοιων νόμων, καθώς αυτοί συμβάλλουν στην επίτευξη ενός μέγιστου επιπέδου διαφάνειας και δημοκρατικής νομιμότητας.

Η εφαρμογή της γενικής νομοθεσίας περί προστασίας δεδομένων και, ειδικότερα, ο αντίκτυπος της ευρύτερης νομοθεσίας τείνει να θέτει σημαντικά μεγαλύτερες προκλήσεις στο πλαίσιο των συστημάτων Υγείας. Σύμφωνα με τη γενική νομοθεσία περί προστασίας δεδομένων, η επεξεργασία προσωπικών δεδομένων για σκοπούς υγείας είναι προνομιακή. Αυτό ισχύει όχι μόνο για την επεξεργασία δεδομένων για την προστασία της υγείας («ζωτικό συμφέρον»), αλλά

και για τη χρήση προσωπικών δεδομένων για σκοπούς δημόσιας υγείας (WHO, 2020).

Κατά συνέπεια, η δημόσια υγεία είναι προνομιακή όσον αφορά τη νομική βάση για την επεξεργασία δεδομένων (την αιτιολόγηση δηλαδή), το εύρος των δραστηριοτήτων επεξεργασίας και, ειδικότερα, τη δευτερογενή χρήση προσωπικών δεδομένων για τη διαχείριση των συστημάτων Υγείας.

Στην καθημερινή πρακτική, οι συνέπειες της περαιτέρω νομοθεσίας συχνά δημιουργούν σημαντικά προβλήματα, συμπεριλαμβανομένων, ενδεικτικά, του ePrivacy (όπως τα «cookies» ιστοτόπων), των κανονισμών ασφάλειας κρίσιμης σημασίας ή πληροφορικής. Η εφαρμογή όλων αυτών των νόμων και κανονισμών στην πράξη και η πρόβλεψη των άμεσων και έμμεσων επιπτώσεων στο σχεδιασμό και τη διαχείριση των συστημάτων Υγείας απαιτεί βαθιά κατανόηση του αντικειμένου και σχετική νομική εμπειρογνωμοσύνη.

Οι επαγγελματίες στον τομέα της διαχείρισης πληροφοριών υγείας πρέπει επίσης να γνωρίζουν ότι τα προνόμια που απολαμβάνει η δημόσια υγεία δεν επεκτείνονται στην προστασία της ακεραιότητας και της διαθεσιμότητας των δεδομένων. Εν συντομία, η εξυπηρέτηση ενός αξιέπαινου σκοπού – όπως η προστασία της δημόσιας υγείας – δεν δικαιολογεί τη μείωση των προτύπων ασφάλειας πληροφορικής. Τέτοια προνόμια συνδέονται αυστηρά με τους συγκεκριμένους σκοπούς δημόσιας υγείας και δεν δικαιολογούν τη δευτερεύουσα χρήση δεδομένων για άλλους σκοπούς καθαυτούς. Επιτρέπεται η δημιουργία υποδομών που εξυπηρετούν δευτερεύουσα χρήση δεδομένων, όπως μητρώα ή βιο-τράπεζες, αλλά κάθε περίπτωση δευτερεύουσας χρήσης πρέπει να ελέγχεται για την προστασία των συμφερόντων των υποκειμένων των δεδομένων και της κοινωνίας (European Union Agency for Fundamental Rights, 2018).

Οι σύνθετες και μεγάλης κλίμακας δραστηριότητες επεξεργασίας δεδομένων στον τομέα της δημόσιας υγείας απαιτούν προσεκτικό σχεδιασμό και εκτέλεση. Στο βαθμό που τέτοια συστήματα απαιτούν επεξεργασία προσωπικών δεδομένων, οι κανονισμοί προστασίας δεδομένων απαιτούν από τους υπεύθυνους επεξεργασίας δεδομένων να διασφαλίζουν ότι λαμβάνουν υπόψη ζητήματα απορρήτου και προστασίας δεδομένων κατά τη φάση σχεδιασμού οποιουδήποτε συστήματος,

υπηρεσίας, προϊόντος ή διαδικασίας και στη συνέχεια καθ' όλη τη διάρκεια του κύκλου ζωής τους. Η ανάπτυξη και η ενσωμάτωση λύσεων προστασίας δεδομένων στις πρώτες φάσεις ενός έργου εντοπίζει τυχόν πιθανά προβλήματα σε πρώιμο στάδιο για την αποτροπή τους μακροπρόθεσμα. Ως εκ τούτου, η υιοθέτηση μιας προστασίας δεδομένων βάσει σχεδιασμού και εξ ορισμού προσέγγισης αποτελεί μέρος της ευθύνης των υπευθύνων επεξεργασίας δεδομένων (European Data Protection Board, 2020).

Η προστασία δεδομένων από προεπιλογή απαιτεί από τους υπεύθυνους επεξεργασίας να διασφαλίζουν ότι επεξεργάζονται μόνο τα δεδομένα που είναι απαραίτητα για την επίτευξη ενός συγκεκριμένου σκοπού. Αυτό συνδέεται με τις θεμελιώδεις αρχές προστασίας δεδομένων της ελαχιστοποίησης δεδομένων και του περιορισμού του σκοπού. Για τον τομέα της δημόσιας υγείας, αυτό δεν οδηγεί σε λύση «default to off», καθώς η αρχή του προεπιλεγμένου σχεδιασμού απαιτεί και πάλι εξισορρόπηση των διακυβευόμενων συμφερόντων και περιορισμό των σκοπών σε ζωτικά συμφέροντα όπως η προστασία και η προαγωγή της υγείας .

Λαμβάνοντας ως παράδειγμα την κατάσταση του COVID-19, η μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων που αφορούν όλους τους πολίτες μπορεί να είναι δικαιολογημένη και απολύτως συμβατή με τις αρχές, στο βαθμό που αυτή η επεξεργασία είναι απαραίτητη για τον μετριασμό του κινδύνου της πανδημίας COVID-19. Ωστόσο, οι αρχές απαιτούν επίσης αποτελεσματικές διασφαλίσεις για να επιτευχθεί το ότι τα προσωπικά δεδομένα δεν χρησιμοποιούνται ή καταχρώνται για δευτερεύοντες σκοπούς εκτός εάν ο δευτερεύων σκοπός είναι εξίσου δικαιολογημένος (όπως η έρευνα με ψευδώνυμα ή ανώνυμα δεδομένα).

Ως εκ τούτου, τα δημόσια ιδρύματα υγείας πρέπει επίσης να επιλέγουν τους εταίρους και τους παρόχους υπηρεσιών προσεκτικά – και, ειδικότερα, τους υπεύθυνους επεξεργασίας δεδομένων και τους υποεπεξεργαστές τους. Οι απαιτήσεις ασφάλειας πληροφορικής και προστασίας δεδομένων θα πρέπει να αποτελούν μέρος οποιασδήποτε σχετικής διαδικασίας διαγωνισμού και προμήθειας, και οι συμβατικές υποχρεώσεις των εταίρων και των παρόχων υπηρεσιών θα πρέπει να αντικατοπτρίζουν όλες τις σχετικές κανονιστικές απαιτήσεις για τον υπεύθυνο επεξεργασίας δεδομένων ή τυχόν πρόσθετες απαιτήσεις που ένας υπεύθυνος

επεξεργασίας δεδομένων κρίνει απαραίτητες – για παράδειγμα, για τον μετριασμό των κινδύνων για τη φήμη ενός οργανισμού Υγείας (WHO, 2020).

Εξάλλου, η νομοθεσία του Ηνωμένου Βασιλείου και της Ευρωπαϊκής Ένωσης για την προστασία δεδομένων απαιτεί η ερευνητική επεξεργασία δεδομένων υγείας να είναι προς το «δημόσιο συμφέρον». Δεν υπάρχουν επεξηγηματικές σημειώσεις και καθοδήγηση για να εξηγηθεί τι σημαίνει ακριβώς αυτό. Ωστόσο, εάν η επεξεργασία της έρευνας περάσει αυτό το τεστ και πληροί το όριο του δημόσιου συμφέροντος, τότε δεν υπάρχει απαίτηση νόμου περί προστασίας δεδομένων για τη συναίνεση ενός υποκειμένου δεδομένων στη χρήση του ή τα προσωπικά της δεδομένα για ερευνητικούς σκοπούς. Συνήθως, εάν η συναίνεση δεν αποτελεί τη νομική βάση για την επεξεργασία, τότε τα υποκείμενα των δεδομένων έχουν το δικαίωμα να αντιταχθούν στην επεξεργασία (Presser et al., 2015).

Εκτός από την παροχή εναλλακτικής λύσης στη συναίνεση ως νόμιμη βάση επεξεργασίας, το δημόσιο συμφέρον χαρακτηρίζει επίσης αυτό το δικαίωμα αντίρρησης όπου η επεξεργασία είναι απαραίτητη για ερευνητικούς σκοπούς. Έτσι, σύμφωνα με τη νομοθεσία του Ηνωμένου Βασιλείου και της Ευρωπαϊκής Ένωσης για την προστασία δεδομένων, το δημόσιο συμφέρον επιτρέπει στους ερευνητές να λειτουργούν με σχετικά μικρό σεβασμό στις ατομικές προτιμήσεις: η ερευνητική χρήση δεδομένων υγείας επιτρέπεται χωρίς ατομική συναίνεση (opt in) ή την ευκαιρία αντίρρησης (opt out). Υπάρχει κίνδυνος η εξασθένιση του ατομικού ελέγχου να επιτρέψει τη χρήση δεδομένων που δεν είναι αποδεκτές από μεμονωμένα υποκείμενα των δεδομένων. Αυτό θα μπορούσε να αυξήσει τη δυσαρέσκεια, να υπονομεύσει την εμπιστοσύνη στην αποτελεσματική διακυβέρνηση και να δυσφημήσει την έρευνα για την υγεία γενικότερα (Taylor, 2014).

Τα τελευταία χρόνια, η κοινή χρήση δεδομένων για την υγεία σπάνια αναδείχτηκε από τον Τύπο. Παρόλο που οι σκοποί της κοινής χρήσης δεν έχουν πάντα δηλωθεί ότι είναι ερευνητικοί σκοποί, η διαμάχη περιέβαλε τις ροές δεδομένων των γενικών ιατρών προς το Κέντρο Πληροφοριών Υγείας και Κοινωνικής Φροντίδας στο πλαίσιο του προγράμματος care.data και της αρχικής κοινής χρήσης δεδομένων συμφωνία μεταξύ της Google Deepmind και του νοσοκομείου Royal Free London (Powles & Hudson, 2017).

Αυτά τα γεγονότα στο Ηνωμένο Βασίλειο έχουν μεγάλο αντίκτυπο στην συζήτηση για την προστασία των προσωπικών δεδομένων στον χώρο της υγείας. Πιο πρόσφατα, η έρευνα επικεντρώθηκε στη ροή δεδομένων υγείας από το Ηνωμένο Βασίλειο προς τις ΗΠΑ, η οποία δημιούργησε σημαντικό θέμα στην δημοσιότητα. Λίγοι θα αμφισβητούσαν πιθανώς την αξία ενός ισχυρού πλαισίου διακυβέρνησης ικανού να προάγει τόσο το δημόσιο συμφέρον για πρόσβαση σε δεδομένα υγείας για κατάλληλους ερευνητικούς σκοπούς, όσο και να προστατεύει και να προωθεί την εμπιστοσύνη του κοινού σε μια εμπιστευτική υπηρεσία υγειονομικής περίθαλψης. Ωστόσο, αυτό θα πρέπει πάντα να γίνεται με στόχο την επίτευξη ισορροπίας μεταξύ ανταγωνιστικών συμφερόντων, γεγονός που είναι ικανό να προάγει και να προστατεύει τη δημόσια υποστήριξη. Η νομική συμμόρφωση από μόνη της δεν θα εξασφαλίσει απαραίτητα την κοινωνική νομιμότητα (Carter et al., 2015).

Η εισαγωγή στον Νόμο για την Προστασία Δεδομένων του 2018 ενός τεστ δημοσίου συμφέροντος, που εφαρμόζεται στην ερευνητική επεξεργασία δεδομένων υγείας, δημιουργεί την ευκαιρία να συμβάλει κανείς περαιτέρω στη δημιουργία ενός πλαισίου που θα υποστηρίζει μόνο κατάλληλες αντισταθμίσεις μεταξύ ανταγωνιστικών συμφερόντων. Πολλά θα εξαρτηθούν από το πώς θα ερμηνευτεί και θα εφαρμοστεί αυτό το νέο τεστ δημοσίου συμφέροντος. Εάν η διασφάλιση που εισήχθη από τον νόμο του 2018 πρόκειται να έχει κάποιο νόημα, τότε πρέπει να είναι δυνατό οι ερευνητικές προτάσεις να αποτύχουν στο τεστ. Ωστόσο, χωρίς μια εφαρμόσιμη έννοια του δημόσιου συμφέροντος είναι αδύνατον να εφαρμοστεί με συνέπεια μια δοκιμή δημοσίου συμφέροντος ικανή να διακρίνει μεταξύ περιπτώσεων έρευνας για την υγεία που είναι προς το δημόσιο συμφέρον από εκείνες που δεν είναι. Είναι επίσης αδύνατο να εξηγηθεί γιατί η δοκιμή δημοσίου συμφέροντος μπορεί να ικανοποιείται σε ένα μέρος της νομοθεσίας για την προστασία δεδομένων, π.χ. σε σχέση με την ανάγκη για νόμιμη βάση, αλλά όχι σε ένα άλλο, π.χ. σε σχέση με την κατάργηση του δικαιώματος αντίρρησης σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (ΕΕ) (GDPR) (Helm Toby, 2019).

Το ζήτημα του ουσιαστικού περιεχομένου του τεστ δημοσίου συμφέροντος στη νομοθεσία ειδικά του Ηνωμένου Βασιλείου για την προστασία δεδομένων είναι σημαντικό όχι μόνο για όσους διεξάγουν έρευνα που υπόκεινται στις διατάξεις του. Μπορεί να ενημερώσει μια κριτική δημοσίου συμφέροντος της νομοθεσίας περί

προστασίας δεδομένων του Ηνωμένου Βασιλείου και της ΕΕ για την προστασία της έρευνας για την υγεία και τον ατομικό έλεγχο της χρήσης και της αποκάλυψης δεδομένων υγείας. Εν κατακλείδι, θα πρέπει να υπογραμμιστεί ότι ο κεντρικός ισχυρισμός, σύμφωνα με τον οποίο ότι το δημόσιο συμφέρον απαιτεί αποδεκτούς λόγους για τυχόν μείωση του ατομικού ελέγχου στη χρήση και αποκάλυψη προσωπικών δεδομένων υγείας. Αυτή η πρόταση παρέχει μια πλατφόρμα για μια κριτική δημοσίου συμφέροντος της νομικής θέσης και του Ηνωμένου Βασιλείου και της ΕΕ, ότι η νομοθεσία περί προστασίας δεδομένων επιτρέπει στους ερευνητές υγείας να επεξεργάζονται ευαίσθητα προσωπικά δεδομένα με σχετικά μικρό σεβασμό στις ατομικές προτιμήσεις.

3.3. Αποτελεσματική αντιμετώπιση του θέματος της προστασίας των προσωπικών δεδομένων των ασθενών και ο ρόλος του εσωτερικού ελέγχου

Οι νόμοι περί προστασίας δεδομένων σε όλο τον κόσμο ακολουθούν μια προσέγγιση προσανατολισμένη στον κίνδυνο και τη διαδικασία για να διασφαλίσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων και την ανθεκτικότητα των συστημάτων. Αυτό απαιτεί μια περιοδική διαδικασία για την επανεξέταση της αποτελεσματικότητας των μέτρων ασφαλείας και τη συνεχή βελτίωσή τους. Η προστασία δεδομένων δεν είναι μια μεμονωμένη δραστηριότητα, αλλά μια εργασία που πρέπει να ενσωματωθεί σε όλες τις δραστηριότητες που σχετίζονται με τη διαχείριση των συστημάτων υγείας. Ομοίως, η προστασία δεδομένων είναι καθήκον και ευθύνη όλων όσων εμπλέκονται στην επεξεργασία δεδομένων και δεν θα πρέπει να ανατίθεται αποκλειστικά σε έναν υπεύθυνο προστασίας δεδομένων ή ένα τμήμα διακυβέρνησης δεδομένων.

Ένα σημαντικό εργαλείο για να διασφαλιστεί ότι όλα τα σχετικά ενδιαφερόμενα μέρη σε έναν οργανισμό αξιολογούν τις απαιτήσεις προστασίας δεδομένων είναι η αξιολόγηση επιπτώσεων στην προστασία δεδομένων (DPIA). Αυτό το επίσημο εργαλείο διαδικασίας και τεκμηρίωσης χρησιμοποιείται ευρέως για δραστηριότητες επεξεργασίας δεδομένων υψηλού κινδύνου και διάφορες αρχές

προστασίας δεδομένων και άλλοι ενδιαφερόμενοι φορείς παρέχουν τέτοια πρότυπα. Συνιστάται μια DPIA πριν από τη δημοσίευση ενός νέου συστήματος πληροφορικής ή μιας δραστηριότητας επεξεργασίας (Wilmslom, 2020).

Οι υπεύθυνοι προστασίας δεδομένων θα πρέπει να είναι στη θέση τους για να καθοδηγούν τον οργανισμό, αλλά η καθημερινή ευθύνη για τη συμμόρφωση με τους νόμους περί προστασίας δεδομένων ανήκει στον υπεύθυνο επεξεργασίας δεδομένων, ως την οντότητα που είναι αρμόδια για την επεξεργασία δεδομένων.

Ως εκ τούτου, η προστασία δεδομένων απαιτεί επαρκείς πόρους, συνεχή εκπαίδευση και υποστήριξη από το υψηλότερο επίπεδο διαχείρισης. Ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει επίσης να διασφαλίζει ότι υπάρχουν διαθέσιμες σχετικές ικανότητες ελέγχου προστασίας δεδομένων και θα πρέπει να είναι σε θέση να υποστηρίζει τους ελέγχους των αρχών προστασίας δεδομένων. Ο έλεγχος προστασίας δεδομένων ορίζεται ως μια συστηματική και ανεξάρτητη εξέταση για να προσδιοριστεί εάν οι δραστηριότητες που περιλαμβάνουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιούνται σύμφωνα με τις πολιτικές και διαδικασίες προστασίας δεδομένων ενός οργανισμού και εάν αυτή η επεξεργασία πληροί τις απαιτήσεις του ισχύοντος κανονιστικού πλαισίου. Το πρόγραμμα ελέγχου θα πρέπει να οδηγεί σε ένα σχέδιο συνεχούς βελτίωσης και μπορεί να οδηγήσει στην ολοκλήρωση προγραμμάτων πιστοποίησης του κλάδου, όπως το ISO 27001 ή το ISO 27701 (Lachaud, 2018).

Η προστασία δεδομένων αποτελεί σημαντικό στοιχείο της ανθρωποκεντρικής προσέγγισης της τεχνολογίας και πυξίδα για τη χρήση της τεχνολογίας στην ψηφιακή μετάβαση των οικονομιών και στη χάραξη πολιτικής. Σε ένα σύστημα δημόσιας υγείας που βασίζεται όλο και περισσότερο στην επεξεργασία προσωπικών δεδομένων, οι νομικές εγγυήσεις που τονίζονται παραπάνω αποτελούν ουσιαστικό εργαλείο για να διασφαλιστεί ότι τα άτομα έχουν καλύτερο έλεγχο των προσωπικών τους δεδομένων και ότι αυτά τα δεδομένα υποβάλλονται σε επεξεργασία για νόμιμο σκοπό, με νόμιμο, δίκαιο και διαφανή τρόπο. Καθώς η προστασία των δεδομένων πρέπει να ενσωματωθεί στο σχεδιασμό και την εκτέλεση προγραμμάτων δημόσιας υγείας, αυτό απαιτεί εκπαίδευση και ενδυνάμωση τόσο των πολιτών όσο και των επαγγελματιών της δημόσιας υγείας.

Η ικανότητα δεδομένων, συμπεριλαμβανομένης της διακυβέρνησης της επεξεργασίας δεδομένων και της προστασίας των προσωπικών δεδομένων, πρέπει να γίνει αναπόσπαστο μέρος των προσόντων των επαγγελματιών δημόσιας υγείας που εργάζονται σε συστήματα υγείας.36 Αυτή η εκπαίδευση πρέπει να βασίζεται στις αρχές που περιγράφονται, αλλά θα πρέπει επίσης να καλύπτει το ισχύον ρυθμιστικό πλαίσιο. Σημαντικό στοιχείο είναι η συνεχής κατάρτιση των επαγγελματιών που έχουν ήδη περάσει την περίοδο της ακαδημαϊκής εκπαίδευσης. Απαιτούνται εργαστήρια, πρακτικές ασκήσεις και μάθηση βάσει προβλημάτων για να λυθούν τα εμπόδια μεταξύ της δημόσιας υγείας και της προστασίας δεδομένων (González Fuster & Kloza, 2016).

Η συνεχής εκπαίδευση είναι επίσης ζωτικής σημασίας για να μπορέσουν οι επαγγελματίες της δημόσιας υγείας να συμβαδίζουν με τον ρυθμό εφαρμογής νέων τεχνολογιών, όπως το cloud computing ή τα συστήματα που βασίζονται σε blockchain. Απαιτείται ενδυνάμωση για να μπορέσουν να εφαρμοστούν σωστά τις αρχές της προστασίας δεδομένων στο σημερινό, διαρκώς μεταβαλλόμενο τεχνολογικό τοπίο.

Ως μέρος της αρχής της λογοδοσίας, η προστασία δεδομένων απαιτεί από κάθε υπεύθυνο επεξεργασίας δεδομένων να αναλάβει την ευθύνη για τις δραστηριότητές της επεξεργασίας και για το πώς συμμορφώνεται με τις αρχές προστασίας δεδομένων. Η ύπαρξη κατάλληλων μέτρων και αρχείων για την απόδειξη της συμμόρφωσης είναι κρίσιμης σημασίας. Μια άλλη βασική απαίτηση είναι ο εσωτερικός και εξωτερικός έλεγχος. Αυτή η δομή ελέγχου μπορεί να πάρει διαφορετικό σχήμα ή μορφή ανάλογα με την ισχύουσα νομοθεσία. Διάφοροι νόμοι περί προστασίας δεδομένων ορίζουν ότι πρέπει να καθιερωθεί η θέση ενός υπευθύνου προστασίας δεδομένων ή υπευθύνου προστασίας προσωπικών δεδομένων. Αυτός είναι ένας ανεξάρτητος ρόλος σε έναν οργανισμό που παρέχει συμβουλές στον υπεύθυνο επεξεργασίας δεδομένων, διατηρεί τα αρχεία των δραστηριοτήτων επεξεργασίας και χρησιμεύει ως σημείο εισόδου για τα υποκείμενα των δεδομένων και τις αρχές (European Commission, 2017).

Ο υπεύθυνος προστασίας δεδομένων διευθύνει επίσης δραστηριότητες ελέγχου, τόσο εντός όσο και σε τρίτους που επεξεργάζονται δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας δεδομένων. Η λειτουργία ελέγχου του

υπεύθυνου προστασίας δεδομένων υποστηρίζεται τακτικά από δυνατότητες εσωτερικού ή εξωτερικού ελέγχου ΤΠ. Είναι σημαντικό ότι ένας υπεύθυνος προστασίας δεδομένων δεν θα πρέπει να έχει καμία σύγκρουση συμφερόντων και θα πρέπει να αναφέρεται στο ανώτατο διοικητικό επίπεδο του οργανισμού.

Η πλειονότητα των χωρών στην Ευρωπαϊκή Ένωση έχουν δημιουργήσει ειδικές αρχές προστασίας δεδομένων και ορισμένες κάνουν διαφοροποίηση μεταξύ των αρχών που επιβλέπουν δημόσιους ή ιδιωτικούς φορείς. Χρησιμοποιώντας τις καταστατικές της εξουσίες, μια αρχή προστασίας δεδομένων θα εξετάζει καταγγελίες από τα υποκείμενα των δεδομένων σε σχέση με πιθανές παραβιάσεις της νομοθεσίας περί προστασίας δεδομένων, θα διεξάγει έρευνες και αναλύσεις σχετικά με παραβιάσεις της νομοθεσίας περί προστασίας δεδομένων και θα λαμβάνει μέτρα επιβολής όπου χρειάζεται και θα προωθεί την ευαισθητοποίηση σχετικά με τα δικαιώματα των δεδομένων δίνοντας την δυνατότητα στους πολίτες να προστατεύουν τα προσωπικά τους στοιχεία σύμφωνα με την ισχύουσα νομοθεσία περί προστασίας δεδομένων (WHO, 2020).

Οι αρχές δημόσιας υγείας θα πρέπει να έχουν υπόψη τους ότι οι κίνδυνοι που συνδέονται με τις παραβιάσεις της προστασίας δεδομένων είναι πολλαπλοί, με πρωταρχικό κίνδυνο τη βλάβη της φήμης τους. Επιπλέον, οι αρχές δημόσιας υγείας και τα ερευνητικά ιδρύματα μπορεί να υπόκεινται σε χρηματικά πρόστιμα (στην περίπτωση του GDPR έως 20 εκατ. ευρώ) ή σε διαταγή ή έκκληση για αποκατάσταση από αρχή προστασίας δεδομένων.38 Προφανώς, αυτό απαιτεί σταθερή προστασία δεδομένων και διαχείριση κινδύνου σε οποιοδήποτε μεγαλύτερο δημόσιο ίδρυμα υγείας – ως εκ τούτου, απαιτείται εξειδικευμένη γνώση στη διασύνδεση μεταξύ συμμόρφωσης, πληροφορικής και προστασίας δεδομένων. Ένας σημαντικός τρόπος αντιμετώπισης αυτού του κινδύνου είναι η τήρηση αναγνωρισμένων προτύπων και πιστοποιητικών, όπως το ISO 27701 για συστήματα διαχείρισης προστασίας δεδομένων. Καθώς η επιδίωξη τέτοιων πιστοποιητικών μπορεί να είναι επαχθής και απαιτεί την κατανομή επαρκών πόρων, οποιοσδήποτε υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να δημιουργήσει ένα εσωτερικό σύστημα ελέγχου προστασίας δεδομένων που να είναι επαρκές και να αντιστοιχεί στους κινδύνους προστασίας δεδομένων του οργανισμού (WHO, 2020).

4. CASE STUDY: Εσωτερικός έλεγχος και προστασία προσωπικών δεδομένων στο παθολογικό νοσοκομείο Αθηνών Σπηλιοπούλειο «Η Αγία Ελένη».

4.1 Βασικοί ορισμοί σχετικά με τον Γενικό Κανονισμό Προσωπικών δεδομένων

GDPR: Ορισμός και Αρχική Εισαγωγή

Το GDPR είναι ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation GDPR). Στοχεύει στο να προσφέρει στους πολίτες της ΕΕ μια ενιαία και εναρμονισμένη προσέγγιση όσον αφορά την προστασία της ιδιωτικής ζωής στην Ευρωπαϊκή Ένωση. Επιδιώκει να ενισχύσει τα δικαιώματα των πολιτών για την προστασία των δεδομένων τους, όπως ορίζεται στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Η ημερομηνία υποχρεωτικής εφαρμογής του GDPR καθορίστηκε στις 25 Μαΐου 2018.

Έχει εφαρμογή σε όλους τους οργανισμούς (ιδιωτικούς και δημόσιους, κρατικές αρχές, συλλόγους κλπ) που διαχειρίζονται, επεξεργάζονται, αποθηκεύουν και διακινούν δεδομένα προσωπικού χαρακτήρα, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες ή σχετίζονται με οποιουδήποτε είδους υπηρεσίες και αγαθά προς Ευρωπαίους πολίτες.

GDPR: Είναι Κανονισμός ή απλή Οδηγία;

Μια από τις πρώτες αλλαγές σχετικά με το GDPR και μια θεμελιώδης αλλαγή από το προηγούμενο πλαίσιο προστασίας δεδομένων (οδηγία της ΕΕ για την προστασία των δεδομένων - οδηγία 95/46 / ΕΕ) είναι ότι, μετά από πολλές συζητήσεις, το κοινοβούλιο της ΕΕ αποφάσισε ότι το νέο πλαίσιο προστασίας της ιδιωτικής ζωής θα δημιουργηθεί με τη μορφή κανονισμού και όχι οδηγίας, γεγονός που σημαίνει ότι είναι μια δεσμευτική νομοθετική πράξη, που εφαρμόζεται άμεσα σε

όλα τα κράτη μέλη της ΕΕ, εξαλείφοντας την ανάγκη κατάρτισης τοπικών νομοθετικών πράξεων. Ωστόσο, παρά την ανάγκη τοπικής νομοθεσίας, είναι πιθανό να υπάρξουν διαφορές ως προς τον τρόπο με τον οποίο ο κανονισμός ερμηνεύεται και επιβάλλεται σε διάφορα κράτη μέλη. Εκτός από την ανάγκη για ένα κοινό πλαίσιο προστασίας της ιδιωτικής ζωής, η ΕΕ ισχυροποιεί τη θέση της και τη δέσμευσή της σχετικά με την προστασία των προσωπικών δεδομένων των υποκειμένων των δεδομένων της ΕΕ (το υποκείμενο των δεδομένων είναι ένα ζωντανό άτομο στο οποίο αναφέρονται προσωπικά δεδομένα).

GDPR: Τι ισχύει σχετικά με τις Παραβιάσεις δεδομένων και την ασφάλεια;

Εκτός από την εισαγωγή νέων δικαιωμάτων για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, το GDPR της ΕΕ εισάγει, επίσης, νέους κανόνες για παραβιάσεις δεδομένων. Σε σύγκριση με την προηγούμενη οδηγία, το GDPR επιβάλλει υποχρεώσεις τόσο στους υπεύθυνους επεξεργασίας δεδομένων όσο και στους επεξεργαστές δεδομένων. Το GDPR προσφέρει, επίσης, καθοδήγηση και παραδείγματα για να διευκολύνει τους οργανισμούς, να μετριάσουν τον κίνδυνο.

Μεταξύ αυτών είναι:

1. ψευδονοποίηση δεδομένων προσωπικού χαρακτήρα (δηλαδή επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο που δεν μπορεί πλέον να αποδοθεί σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών)

2. την ικανότητα να αποκαθιστά εγκαίρως τη διαθεσιμότητα (και την πρόσβαση) σε προσωπικά δεδομένα, ύστερα από φυσικά ή τεχνικά περιστατικά

3. την ικανότητα διασφάλισης της εμπιστευτικότητας, της ακεραιότητας και της ανθεκτικότητας των συστημάτων επεξεργασίας

4. την προσθήκη διαδικασιών για την εξασφάλιση τακτικού ελέγχου και αξιολόγησης τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας των επεξεργασμένων δεδομένων προσωπικού χαρακτήρα

5. Επιπλέον, οι οργανισμοί πρέπει τώρα να πληρούν τα πρότυπα όταν πρόκειται για παραβιάσεις κοινοποιήσεων. Σε γενικές γραμμές, οι οργανώσεις που έχουν υποστεί παραβίαση δεδομένων, πρέπει, να ενημερώσουν την εποπτική αρχή (ανεξάρτητη δημόσια αρχή που έχει συσταθεί από ένα κράτος μέλος σύμφωνα με το άρθρο 51 του GDPR) «χωρίς αδικαιολόγητη καθυστέρηση» εκτός εάν η παραβίαση δεν θέτει σε κίνδυνο τα υποκείμενα των δεδομένων. Εάν υπάρχει κίνδυνος για τα επηρεαζόμενα άτομα, οι οργανώσεις πρέπει επίσης να το γνωστοποιήσουν στα ενδιαφερόμενα πρόσωπα στα οποία αναφέρονται, και πάλι "χωρίς αδικαιολόγητη καθυστέρηση".

GDPR: Τι πρόστιμα προβλέπονται;

Η κακή διαχείριση των παραβιάσεων δεδομένων, θα τιμωρείται με την υψηλότερη βαθμίδα κυρώσεων βάσει του GDPR.

Ένας άλλος τρόπος για το Ευρωπαϊκό Κοινοβούλιο, να επιβεβαιώσει τη δέσμευσή του για την προστασία της ιδιωτικής ζωής , είναι οι νέες κυρώσεις, οι οποίες είναι σημαντικά υψηλότερες από ό, τι στην προηγούμενη οδηγία.

Οι κυρώσεις και τα πρόστιμα, μπορούν τώρα, να φθάσουν το 4% του συνολικού κύκλου εργασιών της εταιρείας, που βρίσκεται σε παραβίαση.

Η λογική πίσω από τα τεράστια πρόστιμα, που αφορούν την νομοθεσία, είναι αρκετά απλή: οι υψηλότερες κυρώσεις για τη μη συμμόρφωση θεωρούνται ότι οδηγούν σε υψηλότερα επίπεδα συμμόρφωσης.

Θα γίνει όλο και πιο δύσκολο για τις επιχειρήσεις, να αποδεχθούν απλώς ένα ορισμένο επίπεδο κινδύνου, όταν χειρίζονται προσωπικά δεδομένα, επειδή οι ποινές είναι τώρα ιδιαίτερα υψηλές.

4.2 Εισαγωγή στα Πληροφοριακά Στοιχεία του Νοσοκομείου

Το Σπηλιοπούλειο Νοσοκομείο «Η Αγία Ελένη» ξεκίνησε τη λειτουργεία του το 1916 με πρωτοβουλία ιδιωτών και παραχώρηση του χώρου από τη Μητρόπολη Αθηνών. Το 2016 έκλεισε 100 χρόνια λειτουργίας προσφέροντας πλούσιο έργο στο χώρο της Υγείας και μάλιστα στην Πρωτοβάθμια Φροντίδα Υγείας. Το 1938 με τον αναγκαστικό Νόμο 1142/1938 και με τη δωρεά του Χαρ. Σπηλιόπουλου, το νοσοκομείο μετονομάζεται σε Σπηλιοπούλειο Νοσοκομείο «Η Αγία Ελένη» και χτίζεται η 2^{η} Πτέρυγα.

Το Νοσοκομείο διαθέτει μικροβιολογικό/ βιοχημικό/ αιματολογικό εργαστήριο, το οποίο είναι πλήρως εξοπλισμένο με σύγχρονα μηχανήματα (βιοχημικό και αιματολογικό αναλυτή) και καλύπτει όλο το φάσμα των βιοχημικών και αιματολογικών εξετάσεων.
Ακόμη, το ακτινολογικό τμήμα του Νοσοκομείου είναι πλήρως ψηφιακό και καλύπτει όλο το φάσμα των συμβατικών ακτινολογικών εξετάσεων. Τέλος, το Νοσοκομείο διαθέτει και εξωτερικά Ιατρεία.

Σύμφωνα με τα στοιχεία του Νοεμβρίου του 2021 το Σπηλιοπούλειο Νοσοκομείο «Η Αγία Ελένη» απασχολεί συνολικά 69 εργαζομένους και διαθέτει 31 κλίνες με το σύνολο των εξωτερικών ασθενών να υπολογίζονται στους 4.261 ενώ οι εσωτερικοί ασθενείς ανέρχονται στους 205.

Τα συνολικά έξοδα ανήλθαν σε 1.162.815€ με τις φαρμακευτικές δαπάνες να είναι στις 121.510€.

Παρακάτω, παρατίθενται κάποιοι βασικοί Δείκτες του Νοσοκομείου:

Λειτουργικοί Δείκτες Νοσοκομείου:

Πληρότητα: 42%

Ημέρες Νοσηλείας: 4.310

ΜΔΝ: 21,02

Μέσος Ρυθμιστής Εισροής (Ρκ): 29,23

Οικονομικοί Δείκτες:

Κόστος/ εσωτ. Ασθενή: 3.967€

Κόστος/ ημέρα νοσηλείας: 189€

Συνολικά στο Νοσοκομείο έχουν πραγματοποιηθεί:

34.485 εργαστηριακές εξετάσεις

3.128 Απεικονιστικές εξετάσεις

Το Νοσοκομείο, λοιπόν, με παρουσία στο χώρο της υγείας πάνω από 100 χρόνια φιλοδοξεί μέσα από τη συνεχή εξέλιξή του αλλά και τον συνεχή εκσυγχρονισμό του, να προσφέρει υψηλού επιπέδου παροχές υγείας και να καλύπτει τις αυξημένες ανάγκες των πολιτών.

Αντικείμενο της μελέτης μας είναι ο έλεγχος για την προσδοκώμενη εναρμόνιση του Νοσοκομείου με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων. Σκοπός μας είναι, να εντοπίσουμε και να αναγνωρίσουμε τις τεχνολογικές και οργανωτικές ανάγκες του Νοσοκομείου προτείνοντας τα αντίστοιχα μέτρα, που θα βοηθήσουν στην επίτευξη της συνεχούς συμμόρφωσης με τις απαιτήσεις του GDPR.

4.3 Περίληψη και σκοπός της εργασίας

Η συγκεκριμένη μελέτη περίπτωσης ασχολείται με την καταγραφή των ευρημάτων κατά τη διενέργεια εσωτερικού ελέγχου του νοσοκομείου και τον έλεγχο συμμόρφωσης αυτού με το Γενικό Κανονισμό Προσωπικών Δεδομένων (ΕΕ) 679/2016 (GDPR). Από την ακόλουθη καταγραφή των στοιχείων, προκύπτει ότι ο

εσωτερικός έλεγχος είναι ένα εξαιρετικά χρήσιμο εργαλείο στα χέρια της Διοίκησης του νοσοκομείου, ώστε να πετύχει τους στόχους της, οικονομικούς και μη. Προϋπόθεση, βέβαια, όλων των παραπάνω, είναι, η Διοίκηση να μεριμνά για τη συμμόρφωση όλων των τμημάτων ως προς τις συστάσεις, που θα γίνονται.

Το Νοσοκομείο Σπηλιοπούλειο «Η Αγία Ελένη» είναι φορέας παροχής υπηρεσιών υγείας με αυξημένη προσέλευση και διακίνηση ασθενών. Ως εκ τούτου, επεξεργάζεται ένα μεγάλο όγκο δεδομένων προσωπικού χαρακτήρα και πληροφορίες (σε ηλεκτρονικά και φυσικά αρχεία), που μπορούν, να ταυτοποιήσουν φυσικά πρόσωπα, όπως ασθενείς, εργαζομένους, συνεργάτες, προμηθευτές κ.α.

Στα πλαίσια, λοιπόν, της έρευνας στο Νοσοκομείο, πραγματοποιήσαμε επισκόπηση επί των διαδικασιών λειτουργίας και των αρχείων που διατηρούνται στο Παθολογικό Νοσοκομείο Αθηνών Σπηλιοπούλειο «Η Αγία Ελένη». Η έρευνα διενεργήθηκε, επίσης, μέσω συνεντεύξεων με άτομα από τη Διοίκηση, υπαλλήλους γραμματείας, λογιστηρίου, γιατρούς και γενικότερα ανθρώπους, που βρίσκονται σε θέσεις, όπου καθημερινά λαμβάνουν και διαχειρίζονται δεδομένα προσωπικού χαρακτήρα, που χαρακτηρίζονται ως ιδιαιτέρως ευαίσθητα δεδομένα καθώς αφορούν την υγεία του ασθενούς, τα γενετικά και τα βιομετρικά τους στοιχεία.

Ως γενετικά δεδομένα εννοούμε τα δεδομένα προσωπικού χαρακτήρα, που αποκτήθηκαν από την ανάλυση βιολογικού δείγματος και δίνουν πληροφορίες ως προς τη φυσιολογία ή την υγεία του ασθενούς. Ενώ ως βιομετρικά δεδομένα εννοούμε αυτά τα δεδομένα προσωπικού χαρακτήρα, που προκύπτουν μετά από ειδική επεξεργασία και επιτρέπουν την αδιαμφισβήτητη ταυτοποίηση του ασθενούς, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα. Επιπλέον, ως δεδομένα που αφορούν την υγεία, εννοούμε, οποιαδήποτε δεδομένα σχετίζονται και αποκαλύπτουν πληροφορίες σχετικά με τη σωματική ή ψυχική υγεία ενός ασθενούς. Γενικότερα, το Νοσοκομείο διαχειρίζεται και λαμβάνει δεδομένα, που αφορούν την κατάσταση της υγείας του ασθενούς, τρέχουσας αλλά και παρελθούσας.

Κατά την εισαγωγή του ασθενούς στο Νοσοκομείο στα σημεία υποδοχής και εξυπηρέτησης, συγκεκριμένα στη Γραμματεία Εξωτερικών ιατρείων, Επειγόντων περιστατικών, στο τμήμα κίνησης ασθενών αλλά και στις συναντήσεις με τους γιατρούς του Νοσοκομείου, καταγράφονται οι πληροφορίες του φυσικού προσώπου,

όπως για παράδειγμα το ονοματεπώνυμό του, τα στοιχεία της ταυτότητάς του, τα στοιχεία επικοινωνίας, ο αριθμός μητρώου του (ΑΜΚΑ), αλλά και πληροφορίες, που προκύπτουν από εξετάσεις, που έχουν γίνει από μέρους του ασθενούς. Επιπλέον, καταγράφονται πληροφορίες σχετικά με ασθένειες, αναπηρίες, ιατρικό ιστορικό, γνωματεύσεις, φαρμακευτικές αγωγές, στοιχεία προηγούμενων χειρουργικών επεμβάσεων και εγχειρήσεων, προηγούμενη υγειονομική περίθαλψη, κλινικές θεραπείες και γενικότερα οποιεσδήποτε άλλες πληροφορίες ζητηθούν από το ιατρικό προσωπικό, που θα βοηθήσουν στη σωστή διάγνωση και θεραπεία.

Επιπρόσθετα, συλλέγονται και στοιχεία σχετικά με την ασφάλιση του ασθενούς, όπως ασφαλιστική εταιρία, ασφαλιστικό ταμείο, αριθμό μητρώου κ.α για τη διεκπεραίωση των οικονομικών συναλλαγών με το Νοσοκομείο.

Τα προσωπικά δεδομένα, που επεξεργάζεται και αποθηκεύει το Νοσοκομείο λαμβάνονται είτε προφορικά, κατά την άφιξη του ασθενούς στα σημεία υποδοχής και εξυπηρέτησης του Νοσοκομείου (Γραμματεία Εξωτερικών Ιατρείων - Επείγοντα Περιστατικά, Τμήμα Κίνησης Ασθενών), τηλεφωνικά κατά τον προγραμματισμό επίσκεψης ή εξέτασης στο Νοσοκομείο (ονοματεπώνυμο και ημερομηνία/ώρα επίσκεψης ή εξέτασης), συμπληρώνοντας τα έγγραφα, που είναι προορισμένα, να αποτελέσουν τον ιατρικό φάκελο του ασθενούς, μετά από πληροφορίες που δίνει ο ίδιος και από όσα προκύπτουν μετά την εξέταση από τους γιατρούς του Νοσοκομείου, καθώς και τα αποτελέσματα των διαγνωστικών ελέγχων/εξετάσεων που έχουν πραγματοποιήσει, αλλά ακόμα και από τα άτομα που συνοδεύουν ή έχουν νόμιμο δικαίωμα να ενεργούν εκ μέρους του ασθενή εάν είναι κάτω των 16 ετών ή δεν είναι σε θέση να παράσχουν οι ίδιοι αυτά τα στοιχεία.

4.4 Διαδικασίες εσωτερικού ελέγχου στον τομέα της μηχανογράφησης

Αφού, λοιπόν, συγκεντρώθηκαν και καταγράφηκαν όλα εκείνα τα στοιχεία προσωπικού χαρακτήρα, που λαμβάνει και επεξεργάζεται το νοσοκομείο, διενεργήθηκε έλεγχος στον τομέα της μηχανογράφησης και πιο συγκεκριμένα στο υποσύστημα διαχείρισης φαρμάκου – υλικών ιατροβιοτεχνολογίας αναλώσιμων υλικών-ανταλλακτικών και υπηρεσιών, στο υποσύστημα κίνησης ασθενών – τιμολόγησης ασθενών – εξωτερικών ιατρείων – απογευματινών ιατρείων – τ.ε.π, στο υποσύστημα διαχείρισης διαγνωστικών – απεικονιστικών εργαστηρίων L.I.S, R.I.S, PAX και τέλος στο υποσύστημα προμηθευτών, ώστε να καταγραφούν τυχόν αποκλίσεις και εσφαλμένες πρακτικές όσον αφορά τις οδηγίες του Κανονισμού, που πρέπει να ακολουθούνται για την προστασία των δεδομένων.

4.5 Ανάλυση Ευρημάτων

Όπως προέκυψε από την πιο πάνω ανάλυση των συστημάτων του Νοσοκομείου αλλά και μέσα από τις συνεντεύξεις που έγιναν με το προσωπικό, εξάγουμε το συμπέρασμα ότι το ίδρυμα δεν έχει εναρμονιστεί με το νέο νομοθετικό πλαίσιο – κανονισμό 2016/679, της ευρωπαϊκής ένωσης αλλά ούτε έχει προβεί και σε σχετικές ενέργειες προκειμένου να είναι σε θέση να συμμορφωθεί με το νέο Κανονισμό (καταληκτική ημερομηνία 25/05/2018).

4.6 Εισηγητική πρόταση προς τη Διοίκηση του Νοσοκομείου

Κατόπιν, λοιπόν, της ανάλυσης των στοιχείων που είχαμε στη διάθεσή μας, συστήσαμε στη διοίκηση του Νοσοκομείου, να προβεί σε άμεσες ενέργειες προκειμένου, να είναι σε θέση το ίδρυμα, να εναρμονιστεί πλήρως με την προαναφερθείσα νομοθεσία προς αποφυγή μελλοντικών προστίμων – κυρώσεων, που δύναται να επιβληθούν από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Πιο συγκεκριμένα, προτείναμε στη Διοίκηση του Νοσοκομείου, να αναθέσει το έργο αυτό σε μία εξειδικευμένη ομάδα, που θα καλύψει όλες τις απαραίτητες λειτουργικές περιοχές και θα καθοδηγήσει τον οργανισμό προς τη συμμόρφωση τόσο με τις νομικές, όσο και με τις τεχνικές απαιτήσεις ασφάλειας του ΓΚΠΔ.

Ειδικότερα, παραθέτουμε μια συνοπτική περιγραφή των σταδίων και των δράσεων, που πρέπει, να διενεργηθούν από το ίδρυμα στο άμεσο χρονικό διάστημα καθώς και η μεθοδολογία υλοποίησης τους:

Επισκόπηση Διαχείρισης προσωπικών δεδομένων

Τα αποτελέσματα αυτού του σταδίου, θα πρέπει, να βασίζονται σε πληροφορίες, που θα συλλέγονται μέσω της επεξεργασίας υλικού, που θα παρέχεται από τον οργανισμό (εσωτερικές διαδικασίες, κώδικες δεοντολογίας, υπάρχοντα αποθέματα δραστηριοτήτων επεξεργασίας) και σε μεγάλο βαθμό μέσω συνεντεύξεων με βασικά πρόσωπα των οργανωτικών μονάδων. Οι αποκτηθείσες πληροφορίες θα πρέπει να αναλυθούν από συμβούλους ειδικευμένους στη διαχείριση δεδομένων.

Προετοιμασία συνεντεύξεων:

Η προετοιμασία των συνεντεύξεων είναι ιδιαίτερα σημαντική, καθότι η κατάλληλη προετοιμασία είναι η βάση για την επιτυχημένη υλοποίηση του όλου έργου.

Συμμετέχοντες: Σε αυτό το στάδιο θα πρέπει να ορίζονται τα άτομα που θα συμμετέχουν στις συνεντεύξεις. Κριτήριο για την επιλογή των σωστών ατόμων θα

πρέπει να είναι η πληρότητα της κατανόησης των δραστηριοτήτων και λειτουργιών της οργανωτικής μονάδας τους.

Η επιλογή θα πρέπει να περιλαμβάνει άτομα που είναι υπεύθυνα για τις λειτουργίες της μονάδας, και άτομα που γνωρίζουν καλά την πορεία και την καθημερινή δραστηριότητα της μονάδας. Επιθυμούμε να συμμετάσχουν σε αυτή τη διαδικασία τουλάχιστον δύο άτομα ανά μονάδα.

Ερωτηματολόγια. Οι συνεντεύξεις θα πρέπει να βασίζονται σε δομημένα ερωτηματολόγια που θα καλύπτουν όλα τα ζητήματα που πρέπει να αναλυθούν. Οποιοδήποτε υλικό που συνοδεύει συγκεκριμένες απαντήσεις (π.χ. τεκμηριωμένες διαδικασίες) θα μπορεί να παρέχεται κατά τη διάρκεια των συνεντεύξεων ή πριν από τις συνεντεύξεις για να διευκολυνθεί η προετοιμασία.

Πρόγραμμα Συνεντεύξεων. Το πρόγραμμα των συνεντεύξεων θα πρέπει να καταρτίζεται, λαμβάνοντας υπ' όψιν τη διαθεσιμότητα των συμμετεχόντων και την ανάγκη τήρησης του χρονοδιαγράμματος του έργου. Η διάρκεια κάθε συνέντευξης θα πρέπει να είναι περίπου 2-3 ώρες ανάλογα με την έκταση των δραστηριοτήτων

Διενέργεια Συνεντεύξεων

Στη διάρκεια των συνεντεύξεων, θα πρέπει να καταγραφούν οι διαδικασίες επεξεργασίας προσωπικών δεδομένων «ως έχουν».

Συγκεκριμένα θα πρέπει να καταγραφούν τα ακόλουθα στοιχεία:

- Κατηγορίες των προσωπικών δεδομένων που επεξεργάζεται το Νοσοκομείο
- Κατηγορίες των υποκειμένων των προσωπικών δεδομένων
- Ο σκοπός κάθε διαδικασίας επεξεργασίας
- Η νομική βάση κάθε διαδικασίας επεξεργασίας (π.χ εκτέλεση σύμβασης ή συγκατάθεση ή έννομο συμφέρον του Υπεύθυνου Επεξεργασίας ή εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας ή διαφύλαξη ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή τρίτου ή έννομη υποχρέωση)

- Ο ρόλος του νοσοκομείου στη διαδικασία επεξεργασίας (υπεύθυνος επεξεργασίας / συνυπεύθυνος επεξεργασίας / εκτελών την επεξεργασία)
- Οι ενέργειες των εκτελούντων την επεξεργασία στις περιπτώσεις που το νοσοκομείο έχει το ρόλο του Υπεύθυνου Επεξεργασίας
- Η μορφή των δεδομένων (έντυπα / ηλεκτρονικά έγγραφα)
- Οι αποδέκτες στους οποίους αποκαλύπτονται τα προσωπικά δεδομένα
- Πιθανή μεταφορά δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή σε διεθνείς οργανισμούς
- Τα προβλεπόμενα χρονικά όρια για τη διαγραφή των διαφόρων κατηγοριών δεδομένων – εφόσον υπάρχουν
- Τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων.

Επιπλέον, στη διάρκεια των συνεντεύξεων:

- Θα πρέπει να συλλεχθούν επιπρόσθετες πληροφορίες που θα επιτρέπουν τον εντοπισμό των δραστηριοτήτων επεξεργασίας δεδομένων υψηλού κινδύνου
- Ιδιαίτερη προσοχή θα πρέπει να δοθεί στις δραστηριότητες υψηλού κινδύνου, συμπεριλαμβανομένης της πιο εμπεριστατωμένης ανάλυσης της σχετικής νομικής βάσης και της λεπτομερούς χαρτογράφησης των ροών δεδομένων προσωπικού χαρακτήρα στο νοσοκομείο
- Θα πρέπει να συλλέγονται πληροφορίες με σκοπό την εκπόνηση της ανάλυσης αποκλίσεων για κάθε επεξεργασία.

Τα αποτελέσματα κάθε συνέντευξης θα πρέπει να καταχωρηθούν απευθείας στα ηλεκτρονικά έντυπα/ερωτηματολόγια. Για κάθε οργανική μονάδα και για κάθε κατηγορία δεδομένων θα πρέπει να συμπληρωθεί ξεχωριστό έντυπο. Τα δεδομένα θα πρέπει να μεταφερθούν αυτόματα στη βάση δεδομένων των συνεντεύξεων.

Δύο διαφορετικοί σύμβουλοι θα πρέπει να συμμετάσχουν σε κάθε συνέντευξη ώστε (α) να μην αποσπάται η προσοχή των συμμετεχόντων κατά τη διάρκεια της καταχώρησης δεδομένων, (β) μία «δεύτερη οπτική» να είναι διαθέσιμη σε περίπτωση αμφιβολίας.

Στο τέλος των συνεντεύξεων, τα συμπληρωμένα ερωτηματολόγια θα πρέπει να αποσταλούν στους συμμετέχοντες και θα πρέπει να επιβεβαιωθούν οι συλλεχθείσες πληροφορίες και να διορθωθούν πιθανά λάθη.

Ανάλυση δεδομένων των συνεντεύξεων

Οι πληροφορίες που θα έχουν συλλεγεί θα πρέπει να τύχουν επεξεργασίας από τους νομικούς (και τεχνικούς) συμβούλους με σκοπό την ταχύτερη δυνατή εξαγωγή των αποτελεσμάτων. Σε αυτό το στάδιο, η επεξεργασία κάθε κατηγορίας προσωπικών δεδομένων θα πρέπει να εξεταστεί σύμφωνα με τις απαιτήσεις του ΓΚΠΔ, έτσι ώστε να εκτιμηθεί το επίπεδο συμμόρφωσης. Τα θέματα που θα εξετασθούν θα πρέπει ενδεικτικά να περιλαμβάνουν τη «νομιμότητα», τη «διαφάνεια» της επεξεργασίας των προσωπικών δεδομένων, τον περιορισμό του σκοπού της επεξεργασίας, την «ελαχιστοποίηση των δεδομένων», την «ακρίβεια» και τον περιορισμό της περιόδου αποθήκευσης των δεδομένων, τα μέτρα προστασίας δεδομένων κ.λπ.

Επιπλέον, θα πρέπει να αναλυθεί η ετοιμότητα του νοσοκομείου να ανταποκριθεί στα δικαιώματα των υποκειμένων των δεδομένων. Ενδεικτικά αναφέρω, το «δικαίωμα πρόσβασης», το «δικαίωμα στη διόρθωση», το «δικαίωμα στη λήθη», το «δικαίωμα περιορισμού της επεξεργασίας», το «δικαίωμα φορητότητας δεδομένων», το «δικαίωμα εναντίωσης».

1. **Έλεγχος Νομικής και Κανονιστικής Συμμόρφωσης**

Διενέργεια Ελέγχου

Ο σκοπός του Νομικού ελέγχου είναι να διερευνηθεί η νομική βάση αναφορικά με την επεξεργασία των Προσωπικών Δεδομένων, να εξεταστεί ο σεβασμός των Αρχών του Γενικού Κανονισμού σε κάθε είδος επεξεργασίας Προσωπικών Δεδομένων, να εντοπιστούν σημεία απόκλισης από τις απαιτήσεις του κανονισμού, να εντοπιστούν συμβάσεις, έγγραφα ενημέρωσης και έγγραφα

συναίνεσης που θα πρέπει να τροποποιηθούν, καθώς επίσης θα πρέπει να παρέχει νομικές συμβουλές για την εξισορρόπηση των δικαιωμάτων του υποκειμένου των προσωπικών δεδομένων και του υπεύθυνου επεξεργασίας.

Συμπερασματικά, οι δραστηριότητες που θα εκτελεστούν στη διάρκεια του νομικού ελέγχου θα πρέπει να περιλαμβάνουν, μεταξύ άλλων:

- Νομικός έλεγχος όλων των καθορισμένων εσωτερικών πολιτικών και διαδικασιών προστασίας προσωπικών πληροφοριών.

- Νομικός έλεγχος υποδειγμάτων συμβάσεων εργασίας ώστε να εξεταστεί εάν καλύπτεται επαρκώς η επεξεργασία προσωπικών δεδομένων των εργαζομένων.

- Νομικός έλεγχος των τυποποιημένων εντύπων συγκατάθεσης που χρησιμοποιούνται για τη συλλογή και την καταγραφή της συγκατάθεσης του υποκειμένου των δεδομένων για την επεξεργασία προσωπικών πληροφοριών.

- Νομικός έλεγχος υποδειγμάτων συμβάσεων με τρίτους (προμηθευτές, συνεργάτες) για τον εντοπισμό τυχόν ελλείψεων σε σχέση με τις σχετικές ρήτρες προστασίας δεδομένων. Εάν δεν χρησιμοποιούνται τυποποιημένες συμβάσεις, η επανεξέταση θα πρέπει να καλύπτει βασικές δραστηριότητες, οι οποίες θα πρέπει τουλάχιστον να περιλαμβάνουν όλες τις συμβάσεις που σχετίζονται με προσδιορισμένες δραστηριότητες επεξεργασίας υψηλού κινδύνου.

- Έλεγχος συμβάσεων βάσει των οποίων το νοσοκομείο επεξεργάζεται προσωπικά δεδομένα ενεργώντας ως Εκτελών την επεξεργασία για λογαριασμό τρίτων Υπεύθυνων επεξεργασίας προσωπικών δεδομένων.

- Έλεγχος των καθορισμένων περιόδων διατήρησης ανά κατηγορία προσωπικών δεδομένων για διάφορους λόγους, όπως για λόγους συμμόρφωσης με νομικές υποχρεώσεις, για έρευνες σε ελεγκτικές αρχές, για νομικές αξιώσεις, για δημόσιο συμφέρον κ.λπ.

- Έλεγχος κειμένων ενημέρωσης των υποκειμένων των δεδομένων στο πλαίσιο της υποχρέωσης διαφάνειας.

2. Έλεγχος Τεχνικής Συμμόρφωσης

Ο σκοπός του ελέγχου τεχνικής συμμόρφωσης θα πρέπει να είναι (α) να προσδιορίσει τις δυνατότητες επεξεργασίας του νοσοκομείου, και (β) να κατανοήσει τις πολιτικές και τις διαδικασίες των πληροφοριακών συστημάτων, (γ) να αξιολογήσει την αποτελεσματικότητα των μέτρων προστασίας προσωπικών δεδομένων που εφαρμόζει το νοσοκομείο.

Για την εκπλήρωση του σκοπού αυτού θα πρέπει να εξεταστούν η Αρχιτεκτονική του Δικτύου και η Διακυβέρνηση (επικσόπηση περιβάλλοντος) Πληροφοριακών Συστημάτων και Ασφάλειας

3. Εξέταση Αρχιτεκτονικής Δικτύου

Θα πρέπει να αξιολογηθεί η ασφάλεια της αρχιτεκτονικής του δικτύου που χρησιμοποιεί το νοσοκομείο καθώς και της υποδομής. Στο πλαίσιο αυτό θα πρέπει να εξεταστούν τα υφιστάμενα διαγράμματα δικτύου και να αξιολογηθεί η λειτουργία, η τοποθέτηση και τα κενά των υφιστάμενων ελέγχων ασφάλειας.

Θα πρέπει να εντοπιστούν τα τυχόν κενά στην προστασία των πληροφοριακών στοιχείων και τα αποτελέσματα να αξιολογηθούν σε συνάρτηση με τις προτεινόμενες βέλτιστες πρακτικές και με όσα συναντώνται συνήθως σε αντίστοιχους φορείς.

Βάσει των πορισμάτων της αξιολόγησης, θα πρέπει να παρέχονται στρατηγικές συστάσεις στο νοσοκομείο για τους τομείς που χρήζουν βελτίωσης.

4. Επισκόπηση του Περιβάλλοντος Πληροφορικής και Ασφάλειας

Σκοπός της Επισκόπησης του Περιβάλλοντος Πληροφορικής και Ασφάλειας (IT and Security Governance Review) θα πρέπει να είναι να εξακριβωθεί εάν ακολουθείται ένας κώδικας δεοντολογίας για τη λειτουργία των συστημάτων IT και θα πρέπει να αξιολογηθεί η αποτελεσματικότητα των τεχνικών και οργανωτικών μέτρων για την προστασία των προσωπικών δεδομένων.

Ο σκοπός της ενέργειας αυτής θα πρέπει να είναι (α) να γίνει κατανοητή η τοπολογία των εγκατεστημένων συστημάτων πληροφορικής που συμμετέχουν στην

επεξεργασία προσωπικών δεδομένων, (β) να γίνουν κατανοητές οι πολιτικές και οι διαδικασίες λειτουργικής διαχείρισης των συστημάτων πληροφορικής και (γ) να αποτιμηθούν τα τεχνολογικά μέσα με τα οποία το νοσοκομείο προστατεύει τα δεδομένα του.

Στη διάρκεια της αξιολόγησης των παρακάτω θεμάτων θα πρέπει να εξετασθούν:

Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)

Θα πρέπει να εξεταστούν για παράδειγμα: η ύπαρξη αρχείων εγκεκριμένων και κοινοποιημένων διαδικασιών, ο σκοπός αυτών, η ύπαρξη Στρατηγικής Διαχείρισης Κινδύνων, ύπαρξη σχεδίων αντιμετώπισης των κινδύνων, περιοδικοί έλεγχοι και βελτιώσεις ανάλογα με τα ευρήματα, κ.λ.π.

Αρμοδιότητες Διοίκησης

Θα πρέπει να εξεταστούν για παράδειγμα: η δέσμευση της Διοίκησης του Νοσοκομείου για να παρέχει τους κατάλληλους πόρους για τη λειτουργία και την ασφάλεια του περιβάλλοντος πληροφορικής, κανονιστικές ρυθμίσεις, απαιτήσεις που πηγάζουν από συμβόλαια, η εξισορρόπηση της λειτουργίας και της ασφάλειας με τις επιχειρηματικές απαιτήσεις, προγράμματα εκπαίδευσης με σκοπό να μειωθεί το κενό μεταξύ των υπαρχουσών και των απαιτούμενων ικανοτήτων του προσωπικού, κ.λ.π.

Εσωτερικοί Έλεγχοι, Ανασκοπήσεις της Διοίκησης, Βελτιώσεις

Θα πρέπει να εξεταστούν για παράδειγμα: περιοδικοί έλεγχοι της διακυβέρνησης του περιβάλλοντος πληροφορικής, εκτίμηση κινδύνων, σχέδια αντιμετώπισης των τα οποία να είναι συμμορφωμένα με τους ισχύοντες νόμους και τους κανονισμούς, τις απαιτήσεις που πηγάζουν από συμβόλαια, κ.λ.π.

Πολιτική Ασφαλείας

Θα πρέπει να εξεταστεί για παράδειγμα, αν υπάρχει πολιτική ασφάλειας εγκεκριμένη από τη διοίκηση του Νοσοκομείου, αν έχει επικοινωνηθεί σε όλο το προσωπικό και τους εξωτερικούς συνεργάτες, αν επικαιροποιείται μετά από μεγάλες αλλαγές ή σοβαρά περιστατικά, κ.λ.π.

Οργάνωση της Ασφάλειας των Πληροφοριών

Θα πρέπει να εξεταστεί για παράδειγμα δέσμευση που περιλαμβάνει μερικά ή όλα από τα παρακάτω: ανάθεση στο προσωπικό, ανακοινώσεις για το προσωπικό, δέσμευση της Διοίκησης, 'Non-Disclosure Agreement' ή 'Confidentiality Agreement' απαραίτητα πριν δοθεί πρόσβαση στα ευαίσθητα στοιχεία της εταιρείας.

Διαχείριση Επικοινωνιών και Λειτουργιών

Θα πρέπει να εξεταστούν για παράδειγμα: καταγεγραμμένες λειτουργικές διαδικασίες, διαδικασίες βασισμένες στην αρχή για γνώση μόνο των απαραίτητων πληροφοριών (need to know), αλλαγές ελέγχων στις εγκαταστάσεις επεξεργασίας πληροφοριών (λογισμικό / υλικό / δίκτυο), διαχωρισμός καθηκόντων, διαχωρισμός μεταξύ δοκιμαστικών συστημάτων και συστημάτων παραγωγής, έλεγχος της υγείας των συστημάτων, διαδικασίας αποδοχής για τα πληροφοριακά συστήματα, διαδικασία προστασίας κατά τη μεταφορά, διαδικασία απόσυρσης αποθηκευτικών μέσων, τεχνικά μέτρα για την προστασία των ιστοσελίδων, καταγραφή όλων των προσβάσεων σε logs, διατήρηση αρχείου όλων των συμβάντων, ύπαρξη διακριτού συστήματος για την καταγραφή των γεγονότων, κ.λ.π.

Έλεγχος Πρόσβασης

Θα πρέπει να εξεταστούν για παράδειγμα: η Πολιτική για τον έλεγχο πρόσβασης, ο περιοδικός επανέλεγχος των δικαιωμάτων πρόσβασης, πολιτικές για τους κωδικούς, επιβολή της πολιτικής για τους κωδικούς με τεχνικούς τρόπους, επιβολή της πολιτική του «clean screen», πρόσθετα μέτρα για την προστασία στις περιπτώσεις της απομακρυσμένης πρόσβασης, κ.λ.π.

Προμήθεια συστημάτων Ασφάλειας Πληροφοριών, Ανάπτυξη και Συντήρησή τους

Θα πρέπει να εξεταστούν για παράδειγμα: ξεκάθαρες απαιτήσεις ασφαλείας για καινούρια έργα, αποτροπή για τη μη εξουσιοδοτημένη εγκατάσταση λογισμικού, ξεκάθαροι ρόλοι και αρμοδιότητες για το ποιος είναι ο υπεύθυνος για το λογισμικό (εγκατάσταση, patch, αναβάθμιση κ.λ.π.), κριτήρια αποδοχής της παραγωγής, πολιτική για τη διαχείριση των patches, κ.λ.π.

Διαχείρισης των περιστατικών ασφαλείας

Θα πρέπει να υπάρχει καταγεγραμμένη και κοινοποιημένη διαδικασία που εγγυάται την έγκαιρη αναφορά των περιστατικών παραβίασης ασφαλείας, τη διαχείριση των περιστατικών ασφάλειας, τη διόρθωση των εντοπιζόμενων αδυναμιών ασφάλειας, τον εντοπισμό των κύριων αιτίων των περιστατικών, κ.λ.π

Απόκτηση, ανάπτυξη και συντήρηση του συστήματος πληροφοριών

Θα πρέπει να υπάρχουν ξεκάθαρες απαιτήσεις ασφαλείας για νέα project, αποτροπή από την εγκατάσταση μη-εγκεκριμένου λογισμικού, σαφείς διαδικασίες ρόλων και ευθυνών προσδιορίζοντας ποιος είναι εξουσιοδοτημένος να αλλάζει λογισμικό παραγωγής (εγκατάσταση, σύνδεση, αναβάθμιση…κλπ), κριτήρια αποδοχής παραγωγής, patch management policy, κλπ

Διαχείριση περιστατικών διαχείρισης πληροφοριών

Θα πρέπει να υπάρχει τεκμηριωμένη και κοινοποιημένη διαδικασία για την εξασφάλιση της έγκαιρης αναφοράς των γεγονότων ασφαλείας, για τον καθορισμό των αδυναμιών ασφαλείας που έχουν αναφερθεί, για την αντιμετώπιση των αναφερόμενων περιστατικών ασφάλειας, για την αναγνώριση της αιτίας των συμβάντων κλπ.

Διαχείριση της συνέχειας της επιχείρησης

Τέλος, θα συστήναμε την ύπαρξη σχεδίων Business Continuity (BC) και Disaster Recovery (DR), περιοδική αναθεώρηση των σχεδίων, εφεδρική εγκατάσταση με επαρκή χωρητικότητα σε σύγκριση με την πρωταρχική, κλπ.

5. Συμπεράσματα

Στόχος της εργασίας αυτής ήταν μέσα απο την βιβλιογραφική επισκόπηση να αναδειχτεί η τήρηση του απορρήτου των προσωπικών δεδομένων των ασθενών του Σπηλιοπούλειου Νοσοκομείου «Η Αγία Ελένη» μέσα από τη διαδικασία εσωτερικού ελέγχου.

Ο εσωτερικός έλεγχος διαμορφώνεται με τέτοιο τρόπο ώστε να υπάρχει σωστή διαχείριση στο σχηματισμό, την οργάνωση και την εκτέλεση ενεργειών για τη διασφάλιση της επίτευξης των στόχων. Με αυτόν τον τρόπο επιτυγχάνεται η πρόληψη, ο εντοπισμός και η διόρθωση ατοπημάτων και λειτουργεί βοηθητικά ώστε η διοίκηση να παραμείνει συγκεντρωμένη στους στόχους της.

Κατ’επέκταση, ο εσωτερικός έλεγχος είναι ένα σημαντικό εργαλείο στα χέρια της διοίκησης για τον έλεγχο και την τήρηση του νέου Κανονισμού για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα. Οι υπεύθυνοι προστασίας δεδομένων (DPO), λοιπόν, θα πρέπει να είναι εξοπλισμένοι με όλα εκείνα τα εργαλεία και τις γνώσεις, που θα τους βοηθήσουν να εμποδίσουν την παραβίαση των προσωπικών δεδομένων.

Ο χώρος της Υγείας είναι ένας κλάδος όπου διαχειρίζεται και έρχεται αντιμέτωπος καθημερινά με την καταγραφή και τήρηση ενός μεγάλου όγκου ευαίσθητων προσωπικών δεδομένων. Γι’ αυτό το λόγο χρήζει ιδιαίτερης σημασίας η διοίκηση του Νοσοκομείου να κατανοήσει οτι μέσα από την ορθή τήρηση του κανονισμού, προσθέτει αξία και παρέχει ιατρικές υπηρεσίες υψηλού επιπέδου. Είναι σημαντικό, λοιπόν, όλες οι δομές Υγείας να κατανοήσουν την σημαντικότητα της εναρμόνισής τους προς τον Κανονισμό αυτό και να μην αρκεστούν σε απλή τυπική συμμόρφωση.

Συγκεκριμένα, μέσα από τη μελέτη περίπτωσης για το Παθολογικό Νοσοκομείο Αθηνών Σπηλιοπούλειο «η Αγία Ελένη», συμπεραίνουμε ότι το νοσοκομείο αυτό δεν ήταν πλήρως εναρμονισμένο με τον Κανονισμό περί Προστασίας Προσωπικών Δεδομένων. Γι’αυτό το λόγο, προτάθηκε στη Διοίκηση του Νοσοκομείου η ανάθεση του έργου σε μία εξειδικευμένη ομάδα που θα τους καθοδηγήσει προς την επίτευξη αυτού του στόχου. Προτάθηκε επίσης, η συνεχής επιμόρφωση του προσωπικού ως προς τις αρχές που διέπουν τον Κανονισμό, καθώς και η απόκτηση κατάλληλων

υποδομών και εξοπλισμού για να αποφευχθούν τυχόν κενά στην προστασία των πληροφοριακών στοιχείων.

Βιβλιογραφία

Abbott, L.J., Daugherty, B., Parker, S., Peters, G.F., (2016). Internal audit quality and financial reporting quality: the joint importance of independence and competence. J. Acc. Res. 54 (1), 3–40.

Al-Matari, A., Al-Swidi, F., Fadzil, D. (2014). The effect of the internal audit and firm performance: A proposed research framework, Int. Rev. Manage. Mark. 4 (1) 34.

Al-Waely, D. (2019). The Impact of Careful Application of Growth Management Policies and Sustainable Development on the Changing Marketing Environment. Eur. J. Econ. Stud. 8, 3–18.

Arens AA, Elder R, Beasley M. (2003). Auditing and assurance services. New Jersey.

Ashbaugh-Skaife, H., Collins, D., & Kinney, W., Jr. (2007). The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. Journal of Accounting and Economics, 44, 166–192.

Association of Healthcare Internal Auditors. (2015). Priorities for Internal Auditors in U.S. Healthcare Provider Organizations. Chief Concerns Include Cybersecurity, Regulatory Compliance and Fraud. New York

Bogle, A. (2018). Health Service Providers Suffer the Most Data Breaches, as Overall Numbers Jump; ABC Science: Sydney.

Bohigas L, Heaton C. (2000). Methods for external evaluation of health care institutions. Int J Qual Health Care.12: 231–238.

Boritz, J.E., Lim, J.H., (2008). IT control weaknesses, IT governance and firm performance. Working paper. University of Waterloo.

Braithwaite J, Coiera E. (2010). Beyond patient safety Flatland. J R Soc Med 103:219–25.

Brink, V., & Witt, H. (1982). Modern internal auditing. New York: John Wiley and Sons

Brown, J. (2000). Labor perspectives on accounting and industrial relations: Historical and comparative review. Labor Studies Journal, 25, 40–74.

Brown, J.R.; Crosno, J.L. (2019). Process and output control in marketing channels: Toward understanding their heterogeneous effects. J. Bus. Ind. Mark. 34, 735–753.

Carrell, M., & Heavrin, C. (2009). Labor relations and collective bargaining: Cases, practice, and law. New Jersey: Prentice Hall.

Carter, P., Graeme T., Dixon-Woods, N. (2015). The social licence for research: Why care.data ran into trouble. Journal of Medical Ethics 41: 404–9.

Chan, K., Farrell, B., & Lee, P. (2008). Earnings management of firms reporting material in- ternal control weaknesses under Section 404 of the Sarbanes-Oxley Act. Auditing: A Journal of Practice & Theory, 27(2), 161–179.

Cheng, L. (2011). Organized labor and debt contracting: Firm-level evidence from collective bargaining. Working paper. The Ohio State University.

Cheng, Q., Goh, B.W., Kim, J.B., (2017). Internal control and operational efficiency. Contemp. Account. Res Forthcoming.

Chevers, D., Lawrence, D., Laidlaw, A., & Nicholson, D. (2016). The Effectiveness of In- ternal Audit in Jamaican Commercial Banks. Accounting and Management Information Systems, 15, 522.

Chornous, G., Ursulenko, G. (2013). Risk management in banks: New approaches. Ekonomika 92, 120–132.

Christopher, J. (2019). The failure of internal audit: Monitoring gaps and a case for a new focus. Journal of Management Inquiry, 28(4), 472–483.

Clinton, S., Pinello, A., & Skaife, H. (2014). The implications of ineffective internal control and SOX 404 reporting for financial analysts. Journal of Accounting and Public Policy, 33, 303–327.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2011. Internal Control—Integrated Framework. December.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2013. Internal Control—Integrated Framework.

Contact Committee of the Supreme Audit Institutions of the European Union. (2019). Audit Compendium. Public health. Audit reports published between 2014 and 2019. Brussels: European Commission.

COSO. Internal Control—Integrated Framework. 2013. Available at: https://www.coso.org/Documents/990025P-Executive- Summary-final-may20.pdf. [15/11/2021].

Deloitte. (2018). The innovation imperative: Forging internal audit's path to greater impact and influence. Deloitte's 2018 Global Chief Audit Executive Research Survey.

Dernarova L, Andrascikova S, Zultzkovz S, Vasilikovz M. (2017) Quality nursing care - a challenge or an unattainable goal? Molisa 5:

Digital Guardian. (2018). Data Insider.. Available at: https://digitalguardian.com/blog/history-data-breaches. [15/12/2021].

Dixon N. (2007). Getting clinical audit right to benefit patients: Getting Clinical Audit Right.

Donelson, D., Ege, M., & McInnis, J. (2014). Internal control weaknesses and financial reporting fraud. Working paper. University of Texas at Austin.

Ege, M. (2015). Does internal audit function quality deter management misconduct? Account. Rev. 90 (2), 495–527.

Emark, K. (2009). Training of internal auditors to perform internal audits according to the ISO 9001: 2000 standard.

European Commission. (2017). Guidelines on data protection officers ('DPOs'). Available at: https:// ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048. [26/12/2021].

European Data Protection Board. (2020). European Data Protection Board. Available at: https://edpb.europa.eu/our-work-tools/ our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

European Union Agency for Cyber-security. (2018). Handbook on security of personal data processing. Athens.

European Union Agency for Fundamental Rights (2018). Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights

Feng, M., Li, C., McVay, S.E., Skaife, H.A., (2015). Does ineffective internal control over financial reporting affect a firm's operations? Evidence from Firms' Inventory Management. Account. Rev. 90 (2), 529–557.

FERMA – Federation of European Risk Management Associations. (2011). Risk management standard. Available at: https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-portuguese-version.pdf. [29/12/2021].

Fitriyah, F.K.; Adrianto, Z.; Irawady, C. (2020). The Internal Audit Role in Fraud Detection and Prevention. Int. J. Innov. Creat. Chang. 11, 491–499.

Fulop, M. T., Szekely, S. V. (2017). The evolution of the internal auditing function in the context of corporate transparency. Audit Financial, v. 15, n. 147, p. 440-450.

Furtuna, C., Ciucioi, A. (2019). Internal Audit in the Era of Continuous Transformation. Survey of Internal Auditors in Romania. Audit. Financial. 17, 452–472.

Geoff, K., Iachello, G., Hong, J. (2007). End-User Privacy in Human-Computer interaction. Found. Trends Hum. Comput. Interact. 1, 1–137

Glazebrook, SG, Buchanan J. (2001). Clinical governance and external audit. J Qual Clin Pract. 21:30–3

González Fuster, G, Kloza, D. (2016). The European handbook for teaching privacy and data protection at schools. Brussels: European Commission.

Gubova, K. (2013). Dynamic changes in quality development and their impact on intangible assets. EDAMBA 2013 – proceedings of the international scientific conference for doctoral students and young researchers. Bratislava: Publishing House.

Hanskamp-Sebregts M, Zegers M, Boeijen W. (2013). Effects of auditing patient safety in hospital care: design of a mixed-method evaluation. BMC Health Serv Res 13:226

Havens, T., Christensen, B., Haseley, S. (2020). Adjusting Internal Audit Priorities in Healthcare Organizations Available at: https://www.protiviti.com/US-en/insights/whitepaper-adjusting-internal-audit-priorities-healthcare-organizations. [15/12/2021].

IIA. (2020). Definition of Internal Auditing.. Available at: https://na.theiia.org/standards-guidance/mandatory-guidance/ Pages/Definition-of-Internal-Auditing.aspx. [12/1/2022].

Ivers, N., Jamtvedt, G, Flottorp, S. (2012). Audit and feedback: effects on professional practice and patient outcomes. Cochrane Database Syst Rev. 6:124-135.

Kalieva, M., Ivanchenko, O., Mirgorodskaya, O. (2018). The role of marketing environment and target audiences in the process of territory brand formation. Eur. Res. Stud. 21:63.

Kalloniatis, C., Kavakli, E., Gritzalis, S. (2008). Addressing privacy requirements in system design: The PriS method. Requir. Eng. 13, 241–255

Kamil, O., Ahmed, E.A. (2020). Extent of Adoption of External Auditor on Internal Control in Bank Auditing. Int. J. Innov. Creat. Chang. 10, 612–624.

Kamps, T. (2013). Systematic Chasing for Economic Success: An Innovation Management Approach; Anchor: Hamburg

Kaplan, HC., Brady, PW., Dritz, MC., Hooper, DK., Linam, WM., Froehle, C. (2010). The influence of context on quality improvement success in health care: a systematic review of the literature. Milbank Q. 88: 500–559.

Kares L. (2010). Auditing. Bratislava: Iura edition.

Kedia, S., Luo, S., Rajgopal, S., (2016). Culture of weak compliance and financial reporting risk. Working paper. Rutgers Business School, NUS Business School, and Columbia University.

Kenthapadi, K. (2006). Models and Algorithms for Data Privacy. Ph.D. Thesis. Stanford University, Stanford.

Kilic, I., Kaya, M. (2015). Investment project evaluation by a decision making methodology based on type-2 fuzzy sets, Appl. Soft Comput. 27 399–410,

Kitchenko, O., Kuchina, S. (2019). Enterprise Communication Policy Indicators Analysis as a Part of Marketing Audit. Technol. Audit Prod. Reserves. 3, 51–54.

Kleiner, M., & Bouillon, L. (1988). Providing business information to production workers: Correlates of compensation and profitability. Industrial and Labor Relations Review, 41, 605–617.

Lachaud E. (2018). The General Data Protection Regulation and the rise of certification as a regulatory instrument; Comput Law Secur Rev. 34(2):244–56

Lawrence, A., Minutti-Meza, M., Vyas, D., (2017). Is operational control risk informative of financial reporting deficiencies? Audit. J. Pract. Theor In-Press.

Lee TA. (1984). The nature, scope and qualities of auditing. London: Carlsberg and Hope.

Lima, D. (2014). The impact of internal auditing on organizational performance: The relevance of human resources auditing. Polytechnic Institute of Porto.

Lin, S., Pizzini, M., Vargus, M., Bardhan, I. (2011). The role of the internal audit function in the disclosure of material weaknesses. Account. Rev. 86 (1), 287–323.

Lobo, G., Wang, C., Yu, X., Zhao, Y. (2020) Material Weakness in Internal Controls and Stock Price Crash Risk. J. Account. Audit. Financ. 35, 106–138.

Mateides, A., Dao, J. (2002). Services. Bratislava: Epos.

Mose, A., Syaifuddin, M. (2016). Analysis of Macro and Micro Environment on the Marketing Strategy Formulation and the Influence to the Competitive Advantage (Case Study). Acad. Strateg. Manag. J. 15, 35–41.

Munsif, V., Raghunandan, K., Dasaratha, V.R., (2012). Internal control reporting and audit report lags: further evidence. Audit. J. Pract. Theor. 31 (3), 203–218.

Nagy, L., & Cenker, W. J. (2002). An assessment of the newly defined internal audit function. Managerial Auditing Journal, 17(3), 130–137.

Powles, J.,Hudson, H. (2017). Google DeepMind and healthcare in an age of algorithms. Health and Technology 7: 351–67.

Prawitt, D.F., Smith, J.L., Wood, D.A., (2009). Internal audit quality and earnings management. Account. Rev. 84 (4), 1255–1280.

Presser, L., Hruskova, M., Rowbottom, H., Kancir, J. (2015). Care.data and access to UK health records: Patient privacy and public trust. Technology Science. August 11. Available at: https://techscience.org/a/2015081103. [21/12/2021].

Public Company Accounting Oversight Board (PCAOB) (2004). Auditing standard no. 2, an audit of internal control over financial reporting performed in conjunction with an audit of financial statements. PCAOB.

Public Company Accounting Oversight Board (PCAOB) (2007). Auditing standard no. 5, an audit of internal control over financial reporting that is integrated with an audit of finan- cial statements. PCAOB.

Ribeiro, R. (2020). Risk Management in Public Organizations: norms and international standards used for risk management, process steps and analysis of the regulatory base in Portugal and Brazil. Lisbon: Exlibris Editions, 2020.

RSM. (2017). Health care internal audit: Identifying prevalent risks within your organization.

Secanell, M., Groene, O., Arah, O. (2014). Deepening our understanding of quality improvement in Europe (DUQuE): overview of a study of hospital quality management in seven countries. Int J Qual Health Care 2014;26:5–15

Silvoso, JA. (1972). Report of the Committee on Basic Auditing Concepts. Account Rev;47:15–74.

Simunic, D. A., & Wu, X. (2009). China-Related research in auditing: A review and directions for future research. China Journal of Accounting Research, 2(2), 1–25.

Skaife, H., Veenman, D., & Wangerin, D. (2013). Internal control over financial reporting and managerial rent extraction: Evidence from the profitability of insider trading. Journal of Accounting and Economics, 55, 91–110.

Spencer E, Walshe K. (2009). National quality improvement policies and strategies in European healthcare systems. Qual Saf Health Care. 18 Suppl 1: i22–7.

Taylor, J., Taylor, N. (2014). Health Research Access to Personal Confidential Data in England and Wales: Assessing Any Gap in Public Attitude between Preferable and Acceptable Models of Consent. Life Sciences, Society and Policy 10: 1–24.

The Institute of Internal Auditors Research Foundation. (2011). International Professional Practices Framework. Florida: IIA

The Institute of Internal Auditors. IIA position paper: the three lines of defense in effective risk management and control. Available at: https://www.iia.org.au/sf_docs/default-source/member-services/thethreelinesofdefenseineffective riskmanagementandcontrol_Position_Paper_Jan_2013.pdf?sfvrsn=0. [21/12/2021].

Tkachenko, V., Kwilinski, A., Tkachenko, I., Puzyrova, P. (2019). Theoretical and Methodical Approaches to the Definition of Marketing Risks Management Concept at Industrial Enterprises. Mark. Manag. Innov. 2, 228–238.

Váchal, M., Vochozka, M. (2013). Business management. Grada Publishing: Praha, Czech Republic.

van Gennip, E , Sillevis Smitt P. (2010). The Netherlands Institute for Accreditation of Hospitals. Int J Qual Health Care. 22:445–51

Victorian Auditor-General's Office. (2005). Managing Patient Safety in Public Hospitals. Melbourne: VAGO.

Wagner C, Gulácsi L, Takacs E. (2006). The implementation of quality management systems in hospitals: a comparison between three countries. BMC Health Serv Res 6:50

Walshe, K., Freeman, T., Latham, L., Wallace, L., Spurgeon, P. (2000). Clinical governance: from policy to practice. Birmingham: Health Services Management Centre.

Wang, T., Zhao, C.-T., Chang, D. (2021). An integrated FAHP-MCGP approach to project selection and resource allocation in risk-based internal audit planning: A case study, Comput. Ind. Eng. 152 (2021) 107012.

Weisbaum, H. (2018). The Total Cost of a Data Breach—Including Lost Business—Keeps Growing. NBC News, 31 July 2018. Available at: https://www.nbcnews.com/business/consumer/total-cost-data-breach- including-lost-business-keeps-growing-n895826. [8/1/2022].

Whigham, N. (2020). Health Sector Tops the List as Australians Hit by 300 Data Breaches Since February. Sydney. Available at: news.com.au [8/1/2022].

WHO. (2020). The protection of personal data in health information systems – principles and processes for public health.

Wilmslom, Information Commissioner's Office. (2020). Personal data breaches. Available at: https:// ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ personal-data-breaches/?q=data+breach. [22/12/2021].

Yee, S., Sujan, A., James, K., Leung, J.K., (2008). The perception of the Singaporean internal audit customers regarding the role and effectiveness of internal audit. Asian J. Bus. Acc. 1 (2), 147–174.