ΚΟΙΝΟΠΡΑΞΙΑ: ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ, ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ ΚΑΙ ΕΘΝΙΚΗΣ ΑΡΧΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΓΕΙΑΣ

Project Title:

Deployment of Generic Cross Border eHealth Services in Cyprus

Agreement number: INEA/CEF/ICT/A2015/11S1451

Action No: 2015-CY-IA-0095

Τίτλος: Εκτίμηση Αντίκτυπου σχετικά με την προστασία Δεδομένων - DPIA (Data Protection Impact Assessment), του Εθνικού Σημείου Επαφής για την ηλεκτρονική υγεία (NCPeH)

Release: v5.0

Αρ. Αναφ. Φακέλου: ΠΚ/2018/05/26

Λευκωσία

30 Ιουνίου, 2020

Βασικές Πληροφορίες Έργου

Πληροφορίες Έργου	
Τίτλος Έργου	**NCPeH CY**
Κωδικός Έργου	***2015-CY-IA-0095***
Ιδιοκτήτης Έργου	**ΕΘΝΙΚΗ ΑΡΧΗ ΗΛΕΚΤΡΟΝΙΚΗ ΥΓΕΙΑΣ**
Στοιχεία Επικοινωνίας Συντονιστή έργου	Τμήμα Πληροφορικής, Πανεπιστήμιο Κύπρου, Λεωφόρος Πανεπιστημίου 1 Αγλαντζιά Λευκωσία 2109 ΚΥΠΡΟΣ (+357) 22892697 (+357) 22892701 pattichi@cs.ucy.ac.cy

Ιστορικό αναθεωρήσεων

Αριθμός Έκδοσης	Ημερομηνία	Συγγραφείς	Εκδότης	Σχόλια
0.1	14/05/2018	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης Μόνικα Καλακουτή Δρ Μάριος Νεοφύτου	ΥΥ & ΠΚ	Πρώτο Προσχέδιο
0.2	19/06/2018	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης Μόνικα Καλακουτή Δρ Μάριος Νεοφύτου	ΥΥ & ΠΚ	Δεύτερο Προσχέδιο
0.3	14/09/2018	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης Μόνικα Καλακουτή Δρ Μάριος Νεοφύτου	ΥΥ & ΠΚ	Τρίτο Προσχέδιο
0.4	28/06/2019	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης Δρ Μάριος Νεοφύτου	ΥΥ & ΠΚ	Τέταρτο Προσχέδιο
0.5	30/06/2020	Καθ. Παττίχης Κωνσταντίνος Ηρακλής Κυριακίδης Δρ Μάριος Νεοφύτου	ΥΥ & ΠΚ & ΕΑΗΥ	Τελική Έκδοση

Θεώρηση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Θεώρησης
Δρ Βάσος Σκουτέλλας	Συντονιστής ελέγχου ποιότητας παραδοτέων	07/10/2020

Έγκριση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Έγκρισης
Καθ. Χρίστος Σχίζας	Προέδρος Εθνικής Αρχής Ηλεκτρονικής Υγείας	08/10/2020

Περίληψη

Η Εκτίμηση Αντίκτυπου για την προστασία των δεδομένων (DPIA) μπορεί να χρησιμοποιηθεί για τον εντοπισμό και την επίλυση δυνητικών ζητημάτων σε πρώτο στάδιο και αποτελεί έναν αποτελεσματικό τρόπο για την υιοθέτηση μιας προσέγγισης προστασίας του σχεδιασμού του έργου. Επίσης, ορίζεται ως μια καλής πρακτικής και απαραίτητη διαδικασία που υποστηρίζει τις πιο κάτω δράσεις:

- Εφαρμογές νέας τεχνολογίας,
- Επεξεργασία δεδομένων που παρουσιάζει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων,
- Μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων συναφών με ιατρικά δεδομένα και μητρώα,
- Μεγάλης κλίμακας συστηματική χρήση ιατρικών βάσεων δεδομένων, κτλ

Η Εκτίμηση Αντίκτυπου για την προστασία των δεδομένων θα εξασφαλίσει / βοηθήσει τους χρήστες των συστημάτων της διασυνοριακής περίθαλψης σε ευρωπαϊκό επίπεδο αλλά και σε Εθνικό επίπεδο προσφέροντας ασφάλεια στην διακίνηση των ευαίσθητων δεδομένων τους.

Το εν λόγο κείμενο βασίστηκε στις οδηγίες της ΕΕ https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/impact-assessments_en.

ΠΕΡΙΕΧΟΜΕΝΑ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Σύντμηση	Πλήρης επεξήγηση
CBeHIS	Cross Border electronic Health Information System (Διασυνοριακό ηλεκτρονικό Πληροφοριακό Σύστημα Υγείας)
CEF	Connecting Europe Facility (Συνδέοντας την Ευρώπη)
eD	eDispensation (ηλεκτρονική Εκτέλεση συνταγής)
eP	ePrescription (ηλεκτρονική Συνταγή)
INEA	Innovations & Networks Executive Agency
MTC	Master Terminology Catalogue
NCPeH	National Contact Point electronic Health
PS	Patient Summary
ΓΝΑ	Γενικό Νοσοκομείο Αμμοχώστου
ΕΕ	Ευρωπαϊκή Ένωση
ΙΥ	Ιατρικές Υπηρεσίες
DPIA	Data Protection Impact Assessment
ΚΜ	Κράτος Μέλος
ΟΠΣΥ	Ολοκληρωμένο Πληροφοριακό Σύστημα Υγείας
ΠΚ	Πανεπιστήμιο Κύπρου
ΥΥ	Υπουργείο Υγείας
GDPR	General Data Protection Regulation
DPO	Data protection Officer
ΝΠΔΔ	Νομικά Πρόσωπα Δημοσίου Δικαίου
ΕΣΙΥ	Εθνικό Συνοπτικό Ιστορικό Υγείας
AD	Active Directory

1. Εισαγωγή και Νομική Βάση επεξεργασίας[1]

Με την έναρξη ισχύος του νέου νόμου General Data Protection Regulation (GDPR), Annex LAW 8 Data protection Law, GDPR, ενισχύονται τα δικαιώματα των φυσικών προσώπων που αφορούν την ενημέρωση, την πρόσβαση, την διόρθωση των προσωπικών τους δεδομένων, τον περιορισμό της επεξεργασίας τους, την άρνηση στην επεξεργασία αυτών, την διαγραφή, την μεταφορά και την αποστολή τους.

Ανάλογα με τα πιο πάνω αυξάνονται και οι υποχρεώσεις των υπεύθυνων της επεξεργασίας αυτών των δεδομένων.

Με άξονες την διαφάνεια και την λογοδοσία, ο υπεύθυνος επεξεργασίας έχει την ευθύνη συμμόρφωσης και απόδειξης ορθής τήρησης της διαδικασίας επεξεργασίας των δεδομένων. και αποτελεί υποχρέωση σε όλα τα Νομικά Πρόσωπα Δημοσίου Δικαίου (ΝΠΔΔ) που επεξεργάζονται προσωπικά δεδομένα. Όπου δηλαδή διενεργείται μεγάλης κλίμακας επεξεργασία **ειδικών κατηγοριών δεδομένων**.

Σύμφωνα με την νομοθεσία, ο ιατρός έχει την υποχρέωση να τηρεί ιατρικό αρχείο, σε ηλεκτρονική ή χειρόγραφη μορφή. Το ιατρικό αρχείο περιέχει δημογραφικά στοιχεία και το ιατρικό ιστορικό, καθώς και δεδομένα που συνδέονται με την ασθένεια, την υγεία του, την διάγνωση, τα αποτελέσματα εξετάσεων, την θεραπεία.

Με τον όρο επεξεργασία δεδομένων εννοείται κάθε πράξη που πραγματοποιείται (ηλεκτρονικά ή χειρόγραφα) σε προσωπικά και ευαίσθητα δεδομένα. Η συλλογή, η οργάνωση, η χρήση, η αποθήκευση ακόμα και η διαγραφή προσωπικών δεδομένων ασθενών από οποιοδήποτε επαγγελματία υγείας θεωρείται επεξεργασία δεδομένων.

Με τον GDPR ενισχύονται σημαντικά τα δικαιώματα των ασθενών σχετικά με τα προσωπικά τους δεδομένα. Είναι προφανές, ότι αυξάνονται οι υποχρεώσεις των ιατρών ως υπευθύνων επεξεργασίας, οι οποίοι επιφορτίζονται με την αρχή της λογοδοσίας (άρθρο 5, Annex LAW 8 Data protection Law, GDPR). Η αρχή της λογοδοσίας αναλύεται σε επιμέρους ενέργειες που πρέπει να πραγματοποιεί ο γιατρός, ο οποίος ως υπεύθυνος επεξεργασίας, φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση του με τις γενικές αρχές που προβλέπει ο κανονισμός GDPR.

Επίσης προβλέπεται :

1 http://www.mof.gov.cy/mof/gpo/gpo.nsf/All/0775A29E264A465BC22582470034CE1C/$file/4215%20%205%20%203%202018%20PARARTIMA%20EKTO.pdf

- Όταν η επεξεργασία δεδομένων βασίζεται στην συγκατάθεση του πολίτη / ασθενή, ο υπεύθυνος πρέπει να μπορεί να αποδείξει την συγκατάθεση (χειρόγραφα ή ηλεκτρονικά, e-mail) (άρθρο 7).
- Η υποχρέωση χορήγησης αντιγράφου των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, όταν ο ασθενής το ζητήσει από τον γιατρό του (άρθρο 15).
- Η αρχή της λογοδοσίας που αφορά και τον εκτελούντα την επεξεργασία, ο οποίος επιλέγεται από τον υπεύθυνο επεξεργασίας. Η επεξεργασία διενεργείται κατόπιν γραπτής σύμβασης δεσμευτικής για τον εκτελούντα, ο οποίος επεξεργάζεται τα δεδομένα μόνο σύμφωνα με τις καταγεγραμμένες εντολές του υπευθύνου επεξεργασίας (άρθρο 28).
- Ο γιατρός ως υπεύθυνος επεξεργασίας αλλά και ο εκτελών την επεξεργασία να τηρεί αρχείο δραστηριοτήτων επεξεργασίας (άρθρο 30).
- Η γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα (άρθρο 33). Εντός 72 ωρών από την στιγμή που ο γιατρός αντιλαμβάνεται την παραβίαση οφείλει να την γνωστοποιήσει, αναλυτικά, αιτιολογημένα και τεκμηριωμένα, στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

<u>Ορισμός Υπεύθυνος Προστασίας Δεδομένων (DPO)</u>

Αποτελεί υποχρέωση όλων των ΝΠΔΔ που επεξεργάζονται προσωπικά δεδομένα και όπου διενεργείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων. Έχει την ευθύνη της παρακολούθησης της συμμόρφωσης και των πολιτικών προστασίας προσωπικών δεδομένων του υπευθύνου ή εκτελούντος την επεξεργασία (άρθρο 39).

Η νομική βάση της επεξεργασίας εστιάζεται:

- στο άρθρο 14 της οδηγίας ΟΔΗΓΙΑ 2011/24/ΕΕ ΤΟΥ ΕΥΡΩΠΑΙΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 9ης Μαρτίου 2011 περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης, η οποία έχει εισαχθεί αυτούσια στην εθνική νομοθεσία, Annex LAW 2 Cyprus Law for Cross Boarder Health Care
- το υποκείμενο των δεδομένων θα παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, στη σύμβαση που έχει υπογραφεί από

τα κράτη μέλη (Από το ΥΥ της Κύπρου και την INEA[2] Annex OS 1 CEF INEA Application and Grant Agreement) για την δημιουργία από αρμόδια όργανα του κράτους δομής NCP για ανταλλαγή των δεδομένων.

2. Πεδίο εφαρμογής του DPIA

Η ιδιωτικότητα είναι ένας όρος που έχει λάβει πολλές ερμηνείες με την πάροδο του χρόνου και συχνά σημαίνει διαφορετικά πράγματα σε διαφορετικά πλαίσια. Μπορούν να βρεθούν ποικίλοι ορισμοί και κάθε κουλτούρα και ακόμη και κάθε άτομο έχει διαφορετικές προσδοκίες ως προς το τι αποτελεί εισβολή της ιδιωτικής ζωής. Στο πλαίσιο αυτού του εγγράφου, ο ορισμός DPIA περιλαμβάνει τα θεμελιώδη δικαιώματα που ορίζονται στα άρθρα 7 και 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («Χάρτης») αντίστοιχα, δηλαδή το δικαίωμα στην ιδιωτική ζωή και το δικαίωμα στην προστασία των προσωπικών δεδομένων. Πρέπει να σημειωθεί ότι το πρότυπο σχετίζεται με την προστασία των προσωπικών δεδομένων όπως ορίζεται στην οδηγία 95/46 / ΕΚ.

Με τη διεξαγωγή του DPIA θα επιτευχθούν οι ακόλουθοι στόχοι:

- Το DPIA θα περιγράφει τις προβλεπόμενες διαδικασίες επεξεργασίας, αξιολόγηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα, τα μέτρα που προβλέπονται για την αντιμετώπιση των κινδύνων, διασφαλίσεων, μέτρων ασφαλείας και μηχανισμών για την προστασία των δεδομένων προσωπικού χαρακτήρα και για την απόδειξη της συμμόρφωσης Οδηγία 95/46 / ΕΚ.
- θα βοηθήσει την Εθνική αρχή προστασίας δεδομένων να αξιολογήσει τη συμμόρφωση της επεξεργασίας και, ειδικότερα, τους κινδύνους για την προστασία των δεδομένων προσωπικού χαρακτήρα του υποκειμένου των δεδομένων και τις σχετικές διασφαλίσεις, όταν οι υπεύθυνοι επεξεργασίας δεδομένων τις συμβουλεύονται πριν από την επεξεργασία δεδομένων, σύμφωνα με τη σύσταση της Επιτροπής. Επομένως, το DPIA θα πρέπει να συνδράμει τον υπεύθυνο επεξεργασίας δεδομένων στην απόδειξη συμμόρφωσης με την οδηγία 95/46 / ΕΚ7.

[2] https://ec.europa.eu/inea/en/welcome-to-innovation-networks-executive-agency

3. Οφέλη από την εκτέλεση DPIA

Τα παρακάτω οφέλη προσδιορίζονται με την υλοποίηση του DPIA:

- Αποτροπή δαπανηρών προσαρμογών σε διαδικασίες ή επανασχεδιασμό του συστήματος με την άμβλυνση των κινδύνων ιδιωτικής ζωής και προστασίας δεδομένων.
- Πρόληψη της διακοπής ενός έργου με έγκαιρη κατανόηση των κυριότερων κινδύνων.
- Μείωση των επιπτώσεων της επιβολής του νόμου και της ανάμειξης της εποπτείας.
- Βελτίωση της ποιότητας των προσωπικών δεδομένων (ελαχιστοποίηση, ακρίβεια).
- Βελτίωση των διαδικασιών εξυπηρέτησης και λειτουργίας.
- Βελτίωση της λήψης αποφάσεων σχετικά με την προστασία δεδομένων.
- Την ευαισθητοποίηση σχετικά με την προστασία της ιδιωτικής ζωής εντός του οργανισμού.
- Βελτίωση της σκοπιμότητας ενός έργου.
- Ενίσχυση της εμπιστοσύνης των καταναλωτών, των εργαζομένων ή των πολιτών στον τρόπο με τον οποίο γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα και η προστασία της ιδιωτικής ζωής.
- Βελτίωση της επικοινωνίας σχετικά με την προστασία της ιδιωτικής ζωής και την προστασία των προσωπικών δεδομένων.

4. Στόχος / Ενδιαφερόμενα μέρη

Το Υπουργείο Υγείας, ως η αρμόδια Εθνική αρχή ηλεκτρονικής Υγείας και μέλος της εκτελεστικής εξουσίας της Κυβέρνησης, μαζί με το Πανεπιστήμιο Κύπρου έχουν συμβληθεί και συμμετέχουν στο έργο "Ανάπτυξη διασυνοριακών ηλεκτρονικών υπηρεσιών υγείας στην Κύπρο (“Deployment of Generic Cross Border e Health Services in Cyprus”, action Number 2015-CY-IA-0095)".

Το συγκεκριμένο έργο αποτελεί μέρος του χρηματοδοτουμένου Ευρωπαϊκού έργου, που υλοποιείται στο πλαίσιο του Ευρωπαϊκού Προγράμματος «ΣΥΝΔΕΟΝΤΑΣ ΤΗΝ ΕΥΡΩΠΗ (Connecting Europe Facility – CEF TELECOM)» και το οποίο έχει ξεκινήσει την 01/01/2017 και αναμένεται να ολοκληρωθεί στις 31/12/2020.

Κύριος στόχος του έργου αυτού είναι η υλοποίηση κατάλληλων διασυνδέσεων και διαδικτυακών ηλεκτρονικών υπηρεσιών, οι οποίες θα κάνουν εφικτή την ανταλλαγή

Ηλεκτρονικών Συνταγών Φαρμάκων (ePrescriptions) και του Συνοπτικού Ιστορικού Υγείας (Patient Summary), με σκοπό την επίτευξη των ακόλουθων στόχων:

1. Διασυνοριακή περίθαλψη και ασφαλής πρόσβαση στις πληροφορίες για την υγεία των ασθενών μεταξύ των ευρωπαϊκών συστημάτων υγειονομικής περίθαλψης, ιδίως όσον αφορά την ανταλλαγή του Συνοπτικού Ιστορικού Υγείας ασθενών (Patient Summary) και την Ηλεκτρονική Συνταγογράφηση (ePrescription).
2. Συμβολή στην ασφάλεια των ασθενών, μειώνοντας τη συχνότητα των ιατρικών σφαλμάτων και παρέχοντας γρήγορη πρόσβαση στις πληροφορίες για την υγεία τους.
3. Προσβασιμότητα στις συνταγές του ασθενούς, όταν αυτός βρίσκεται στο εξωτερικό.
4. Παροχή πληροφορίας ζωτικής σημασίας σε επείγουσες καταστάσεις στον επαγγελματία υγείας και
5. Μείωση των επαναλήψεων διαγνωστικών διαδικασιών.

Στόχος της Συνεργασίας ΥΥ και ΠΚ είναι η παροχή υψηλής ποιότητας διασυνοριακής υγειονομικής περίθαλψης στους πολίτες της που διαμένουν στο εξωτερικό, καθώς και σε πολίτες Κρατών Μελών της Ευρωπαϊκής Ένωσης που επισκέπτονται τη χώρα μας. Η νομική βάση επεξεργασίας υποστηρίζεται από την υπογραφή της σύμβασης μεταξύ του ΥΥ της ΕΕ και του ΠΚ, καθώς και από την νομοθεσία για την Ηλεκτρονική Υγεία που καθιστά τη Δημιουργία , φύλαξη και ενημέρωση του ΗΦΑ υποχρεωτική για τους επαγγελματίες Υγείας.

Επιπλέον, τον Οκτώβριο του 2019 ο νόμος περί Ηλεκτρονικής Υγείας έχει εφαρμοστεί καθιστώντας την Αρχή ως ο νόμιμος ιδιοκτήτης των διασυνοριακών υπηρεσιών υγείας. Βάση αυτού έχει συμπεριληφθεί η Αρχή Ηλεκτρονικής Υγείας στην κοινοπραξία του έργου.

5. Ο ρόλος της Αρχής Προστασίας Δεδομένων

Η Αρχή Προστασίας Δεδομένων αποτελεί σημαντικό φορέα κατά την εκτέλεση του DPIA. Η έκθεση DPIA καταρτίζεται κατά τρόπον ώστε Εθνική Αρχή Προστασίας Δεδομένων να μπορεί να παρακολουθεί και να εποπτεύει την επεξεργασία δεδομένων προσωπικού χαρακτήρα με αυστηρό σεβασμό των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών και εγγυήσεων που κατοχυρώνονται στο ρυθμιστικό πλαίσιο της ΕΕ.

Η έκθεση DPIA παρέχεται με την επιφύλαξη των υποχρεώσεων που απορρέουν από την οδηγία 95/46 / ΕΚ για τους υπεύθυνους επεξεργασίας δεδομένων, και ιδίως την

ανεξάρτητη υποχρέωση κοινοποίησης στην αρμόδια αρχή, όπως περιγράφεται στο τμήμα IX της οδηγίας 95/46 / ΕΚ.

Η DPIA έχει σαφή περιγραφή όλων των παραγόντων, των συνιστωσών και των αλληλεπιδράσεων του δικτύου, ούτως ώστε είναι σε θέση να προσδιορίσει με σαφήνεια την ευαισθησία των ανταλλασσόμενων πληροφοριών καθώς και όλες τις ανησυχίες που σχετίζονται με την προστασία της ιδιωτικής ζωής. Κατά την ανάλυση, η Αρχή Προστασίας Δεδομένων θα είναι σε θέση να επαληθεύει όλους τους προσδιορισμένους κινδύνους και να αξιολογεί εάν οι αντίστοιχοι έλεγχοι είναι επαρκείς για την άμβλυνση ή την ελαχιστοποίηση των εντοπισθέντων κινδύνων.

6. Προσωπικά Δεδομένα

6.1 Διαδικασία & Ειδικές Κατηγορίες Δεδομένων.

Όταν ένας πολίτης κάνει μια μη προγραμματισμένη επίσκεψη σε έναν πάροχο υγειονομικής περίθαλψης στην Ευρωπαϊκή Ένωση, ο επαγγελματίας υγείας θα μπορεί να έχει πρόσβαση στο Συνοπτικό Ιστορικό Υγείας του ασθενή, κατόπιν σχετικής συγκατάθεσής του.

Επίσης, οι υπηρεσίες ePrescription και eDispensation δίνουν τη δυνατότητα σε έναν ασθενή που βρίσκεται στο εξωτερικό να λάβει την ισοδύναμη φαρμακευτική αγωγή που θα λάμβανε στη χώρα του. Δηλαδή η υπηρεσία αυτή στοχεύει στην διασυνοριακή εκτέλεση Ηλεκτρονικών Συνταγών και την καταγραφή των φαρμάκων που διανέμονται.

Η Κύπρος περιλαμβάνεται στις χώρες του 'Wave 1' σε ότι αφορά στην υλοποίηση διασυνοριακών υπηρεσιών όπως περιγράφεται στη σύμβαση που έχει υπογραφεί.

Για διάφορους λόγους η Κύπρος έχει μεταφερθεί στο Wave 3.

Το έργο που καλείται να υλοποιήσει έκαστος φορέας υλοποίησης είναι η παροχή εξειδικευμένων υπηρεσιών διασυνοριακής περίθαλψης, καθώς επίσης και ο σχεδιασμός, υλοποίηση και θέση σε παραγωγική λειτουργία όλων των διασυνοριακών υπηρεσιών Συνοπτικού Ιστορικού Υγείας και Ηλεκτρονικής Συνταγογράφησης ως Χώρα Α και Χώρα Β (eP A και eP B), όπως έχουν καθοριστεί στη Συμφωνία Επιχορήγησης με την [3]INEA (Ευρωπαϊκή Επιτροπή) (Grant Agreement -Παράρτημα Α) για το ευρωπαϊκό έργο

[3] https://ec.europa.eu/transport/themes/infrastructure/inea_en

«Ανάπτυξη γενικών διασυνοριακών υπηρεσιών ηλεκτρονικής υγείας» (“Deployment of Generic Cross Border eHealth Services”).

Οι ειδικοί στόχοι του Έργου, που καλείται να εκτελέσει ο φορέας, αναφορικά με τις Δράσεις («Activities») και τις επιμέρους Εργασίες («Tasks»), περιγράφονται στη Συμφωνία Επιχορήγησης («Grant Agreement»)

Μέσα στα πλαίσια του ευρωπαϊκού δικτύου για την ηλεκτρονική υγεία (eHealth Network), του οποίου η Κύπρος είναι μέλος, αποφασίστηκε μεταξύ των Κρατών Μελών του δικτύου, για διευκόλυνση της διασυνοριακής περίθαλψης, η δημιουργία μιας κοινής πλατφόρμας για ανταλλαγή πληροφοριών των ασθενών, με τη μορφή:

1. Συνοπτικού Ιστορικού Υγείας (Patient Summary (PS)) και

2. Ηλεκτρονικής συνταγογράφησης (ePrescription (eP))

Η κοινή πλατφόρμα (Core services) θα αναπτυχθεί από το eHealth Network[4] ενώ κάθε χώρα μέλος θα αναπτύξει το ηλεκτρονικό εθνικό σημείο επαφής eNCP eHealth (generic services) μέσω του οποίου θα αποστέλλονται και θα παραλαμβάνονται συμφωνημένα στοιχεία του Συνοπτικού Ιστορικού Υγείας (PS) και συμφωνημένη μορφή της ηλεκτρονικής συνταγής (eP).

Ο κύριος στόχος αυτής της εφαρμογής είναι η ανταλλαγή των πληροφοριών του ασθενή σε κοινή μορφή και μέσω ενός ασφαλούς δικτύου.

Η ανάπτυξη της πλατφόρμας σε κάθε Κράτος Μέλος (ΚΜ) είναι υποχρέωσή του και θα διασφαλίζει ηλεκτρονικά πλέον το δικαίωμα της ταυτοποίησης και της ασφαλούς πρόσβασης των ασθενών και των παροχών υγειονομικής περίθαλψης σε αναγκαία στοιχεία, ενώ ταξιδεύουν, του Συνοπτικού Ιστορικού Υγείας και της ιατροφαρμακευτικής αγωγής.

Ουσιαστική νομική βάση για την επεξεργασία και τη μεταποίηση των δεδομένων παρέχεται από την νομοθεσία «ΝΟΜΟΣ ΠΟΥ ΤΡΟΠΟΠΟΙΕΙ ΤΟΥΣ ΠΕΡΙ ΤΗΣ ΕΦΑΡΜΟΓΗΣ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΩΝ ΑΣΘΕΝΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΔΙΑΣΥΝΟΡΙΑΚΗΣ ΥΓΕΙΟΝΟΜΙΚΗΣ ΠΕΡΙΘΑΛΨΗΣ ΝΟΜΟΥΣ ΤΟΥ 2013 ΕΩΣ 2016». Annex LAW 2 Cyprus Law for Cross Boarder Health Care

Η συναίνεση του ασθενή ζητείται και δίνεται εγγράφως από τον ίδιο τον ασθενή. Η συγκατάθεση αφορά επίσης την δευτερογενή επεξεργασία των δεδομένων. Η

[4] https://ec.europa.eu/health/ehealth/policy/network_en

συγκατάθεση εμφανίζεται ηλεκτρονικά στο ηλεκτρονικό αρχείο της εφαρμογής και το φυσικό αρχείο της συγκατάθεσης του ασθενή φυλάσσεται στον φυσικό του ΗΦΑ. Η ηλεκτρονική συγκατάθεση σημειώνεται από τον θεράποντα Ιατρό στο σύστημα και φυλάσσεται στο σημείο φύλαξης του Ηλεκτρονικού αρχείου.

Η **δευτερογενής επεξεργασία δεδομένων** πραγματοποιείται από την Εθνική Αρχή ηλεκτρονικής Υγείας η οποία έχει και την νομική ευθύνη ως υπεύθυνου επεξεργασίας, με τον εκτελών την επεξεργασία να είναι το ΠΚ.

Η επεξεργασία δεδομένων προς το παρόν αφορά:

- δεδομένα χρήσης της υπηρεσίας από ασθενείς και γιατρούς καθώς και
- δεδομένα που αφορούν την ταχύτητα, την επάρκεια και την χρησιμότητα της υπηρεσίας.

Τα δεδομένα αυτά αποτελούν συμβατική υποχρέωση των χωρών που συμμετέχουν στο πρόγραμμα.

Σε περίπτωση που η χώρα καταγωγής του ασθενή δεν επιτρέπει την δευτερογενή επεξεργασία των δεδομένων ενώ η χώρα προέλευσης της θεραπείας το επιτρέπει ή έχει χαμηλότερες δικλίδες ασφαλείας τότε ο χειρισμός των δεδομένων διευθετείται από την υπογραφή συμφωνίας μεταξύ των χωρών.

6.2 Αρμοδιότητες

Το Υπουργείο Υγείας είναι η αρμόδια αρχή και ο συγκεκριμένος τομέας παροχής υπηρεσιών τυγχάνει διαχείρισης και διοίκησης από το Υπουργείο Υγείας (Νομικό υπόβαθρο αποτελούν «Ο περί δημοσίας υπηρεσίας και διοίκησης νόμοι καθώς και οι περί ιατρικών ιδρυμάτων νόμοι»), το οποίο είναι αρμόδιο και νομικά υπεύθυνο για τη διασφάλιση της πρόσβασης σε υπηρεσίες υγείας για όλους τους δικαιούχους και χρηματοδοτείται αποκλειστικά από το δημόσιο προϋπολογισμό.

Με την ένταξη στην κοινοπραξία του έργου της Εθνικής Αρχής Ηλεκτρονικής Υγείας και την εφαρμογή του νόμου περί της ηλεκτρονικής υγείας, νομικά υπεύθυνος των διασυνοριακών υπηρεσιών υγείας είναι η Αρχή. Οπότε η ΕΑΗΥ είναι η αρμόδια αρχή για την υλοποίηση και λειτουργία του Εθνικού σημείου επαφής, καθώς έχει προχωρήσει με διοικητική απόφαση για τη δημιουργία της δομής του σχετικού NCPeH με τις κατάλληλες αρμοδιότητες του οποίου το εύρος υπηρεσιών και αναλυτικές αρμοδιότητες περιγράφεται πιο κάτω (βλέπε οργανόγραμμα της ΕΑΥΗ).

Η Εθνική Αρχή ηλεκτρονικής Υγείας διαθέτει την αρμοδιότητα να συμβάλλεται και διαθέτει το αρμόδιο τμήμα (διεύθυνση αγορών και προμηθειών) για την δημοπράτηση, σύναψη και υλοποίηση συμβάσεων όπως προβλέπεται από την σχετική νομοθεσία.

Υπηρεσίες Υγείας

Οι υπηρεσίες υγείας που υπάγονται απευθείας στην διοίκηση και διεύθυνση του ΥΥ, παρέχονται από τα πέντε (5) κύρια περιφερειακά νοσηλευτήρια (ένα από τα οποία θα χρησιμοποιηθεί για την παροχή υπηρεσιών Συνοπτικού Ιστορικού Υγείας) και ένα (1) παιδιατρικό/γυναικολογικό νοσηλευτήριο, δύο (2) μικρά αγροτικά νοσηλευτήρια και είκοσι τρία (23) Κέντρα Υγείας, καθώς επίσης και από διακόσια τριάντα πέντε (235) υπό-κέντρα με περιοδεύοντες ομάδες ιατρών. Επιπλέον, το Υπουργείο εφαρμόζει σχέδιο παροχής οικονομικής αρωγής για υπηρεσίες που δεν προσφέρονται στο δημόσιο τομέα, υπό συγκεκριμένους όρους και προϋποθέσεις.

Στην παρούσα χρονική περίοδο, ο δημόσιος προϋπολογισμός πιέζεται από την αυξημένη ζήτηση υπηρεσιών υγείας από τα δημόσια νοσηλευτήρια, τη στιγμή που η οικονομική κρίση εντείνει τα προβλήματα με αρνητικές συνέπειες για τον ίδιο τον πληθυσμό. Ο ιδιωτικός τομέας παροχής υπηρεσιών υγείας χρηματοδοτείται από τους ίδιους τους ασθενείς και από εθελοντική ασφάλιση υγείας. Οι υπηρεσίες υγείας του τομέα αυτού παρέχονται από κερδοσκοπικού χαρακτήρα νοσοκομεία, πολυκλινικές, κλινικές, διαγνωστικά κέντρα, φαρμακεία και ανεξάρτητους επαγγελματίες, τα οποία υπάγονται στον έλεγχο, ρύθμιση και αδειοδότηση του Υπουργείου Υγείας.

Οι κατηγορίες προσωπικών δεδομένων και ειδικών κατηγοριών, συλλέγονται από τον ίδιο τον ασθενή και στην παρουσία του. Αυτές και οι αλλαγές οι οποίες τροποποιούν τα συγκεκριμένα έγγραφα θα γίνονται στο μέλλον πάντα στην παρουσία του ασθενή, ο οποίος έχει και την ευθύνη επιλογής και συγκατάθεσης για τον συγκεκριμένο γιατρό. Έτσι οποιαδήποτε τροποποίηση λαμβάνει χώρα ενώπιον και εν γνώσει του ασθενή.

6.3 Περιλαμβανόμενα προσωπικά δεδομένα

Η έννοια των προσωπικών δεδομένων ορίζεται στο άρθρο 2 της οδηγίας 95/46. Περαιτέρω καθοδήγηση σχετικά με αυτόν τον ορισμό μπορεί να βρεθεί στη γνωμοδότηση WP136 της ομάδας εργασίας του άρθρου 29 σχετικά με την έννοια των προσωπικών δεδομένων.

Η εν λόγω υλοποίηση θα διαχειρίζεται τρεις ομάδες δεδομένων:

- Δημογραφικά στοιχεία ασθενή ή και – Στοιχεία συνοδού.
- Σταθερά δεδομένα ασθενή (π.χ. Αλλεργίες), δηλαδή δεδομένα ανεξάρτητα κάποιου περιστατικού.

- Στοιχεία εξαρτόμενα από την/τις νοσηλία/-ίες σε κάποιο νοσοκομείο (πχ συνταγογράφηση περιστατικών – εξιτήρια).

Η καταχώρηση των δεδομένων θα γίνεται σε τοπικό επίπεδο (δηλαδή στη βάση του εκάστοτε νοσοκομείου) και σε χρόνο που θα συμφωνηθεί. Μπορεί να γίνει τμηματική καταχώρηση.

Αναλυτικά, τα δεδομένα που θα συντηρούνται αφορούν:

- Δημογραφικά στοιχεία ασθενή – Στοιχεία συνοδού.

  Ειδικές κατηγορίες Δεδομένων:
- Σταθερά δεδομένα ασθενή (π.χ. Αλλεργίες), δηλαδή δεδομένα ανεξάρτητα κάποιου περιστατικού.

  Τα δεδομένα αυτά αφορούν:
  - Allergies
  - Medical Alert
  - Medical History (Vaccinations, List of resolved or inactive problems, Surgical Procedures)
  - Medical Problems
  - Medical Devices and Implants.
  - Social History
  - Diagnostic Tests
  - Pregnacy History
  - Autonomy Invalidity
- Στοιχεία εξαρτόμενα από την/τις νοσηλία /-ίες σε κάποιο νοσοκομείο (πχ συνταγογράφηση περιστατικών – εξιτήρια).
  - Medication Summary
  - Physical Findings
  - Treatment recommendations

Στην περίπτωση μας ο υπεύθυνος της επεξεργασίας είναι η Εθνική Αρχή ηλεκτρονικής Υγείας και ο εκτελών την επεξεργασία το ΠΚ, όπως συνάδει από τη σύμβαση που έχει υπογραφεί.

7. Φύση του Συστήματος

Για την κάλυψη των απαιτήσεων του έργου και προκειμένου να είναι εφικτή η δημιουργία του PS που θα αναπτυχθεί σε πρώτη φάση του έργου, είναι η εφαρμογή καταχώρησης/προβολής ενός συνόλου δεδομένων, το οποίο για τις ανάγκες του έργου θα το

ονομάσουμε «Εθνικό Συνοπτικό Ιστορικό Υγείας (Ε.Σ.Ι.Υ.)», το οποίο θα βασιστεί στις προδιαγραφές του Patient Summary (υιοθετήθηκε από το Ευρωπαϊκό eHealth Network) και θα προσαρμοστεί στα κυπριακά δεδομένα. Ουσιαστικά αφορά στα δεδομένα που θα καταγράφονται ηλεκτρονικά από τους γιατρούς σε πραγματικό χρόνο και με την παρουσία και εξουσιοδότηση του ασθενή. Ο γιατρός θα χρησιμοποιεί μια διαδικτυακή εφαρμογή και θα καταγράφει όλα τα δεδομένα εκτός από κάποια που θα αντλούνται από τη βάση του αρχείου πληθυσμού μέσω του ασφαλούς κυβερνητικού δικτύου.

1) Οι περιλήψεις δεδομένων ασθενών επιτρέπουν την ανταλλαγή πληροφοριών σχετικά με το ιατρικό υπόβαθρο και το ιστορικό ασθενούς από τη χώρα Α (τη χώρα ασφάλισης του ασθενούς) από έναν επαγγελματία υγείας σε άλλο κράτος μέλος Χώρα Β (χώρα θεραπείας).
Το Ιατρικό Ιστορικό είναι ένα αναγνωρίσιμο σύνολο δεδομένων βασικών και κατανοητών πληροφοριών για την υγεία που απαιτούνται για τη διασφάλιση του συντονισμού της υγειονομικής περίθαλψης και της συνέχειας της περίθαλψης.

- Ο ασθενής συμβουλεύεται ένα επαγγελματία υγείας στη χώρα Β
- Ο ασθενής αναγνωρίζεται (αναγνωρισμένη ταυτότητα από τη χώρα Α)
- Ο επαγγελματίας υγείας αναγνωρίζεται, επικυρώνεται και εγκρίνεται στη χώρα Β
- Ο ασθενής μπορεί να έχει δώσει συγκατάθεση πριν ταξιδέψει στη χώρα Β ή στη χώρα Β στον επαγγελματία υγείας (εκτός από περιπτώσεις έκτακτης ανάγκης)

Στην τελευταία περίπτωση, ο επαγγελματίας υγείας θα καταχωρήσει αυτή την επιβεβαίωση.
Η Περίληψη Ασθενών μεταφέρεται ηλεκτρονικά από τη χώρα προέλευσης του ασθενούς στον επαγγελματία υγείας της χώρας στην οποία επισκέπτεται (η "χώρα που επισκέπτεται") με ασφαλή τρόπο. Ο επαγγελματίας υγείας ανακτά την Περίληψη Ασθενούς και το χρησιμοποιεί για τη διαβούλευση.
Το PS λαμβάνεται τόσο στη γλώσσα του ασθενούς (PDF του αρχικού PS) όσο και ως μεταφρασμένη έκδοση για τον επαγγελματία υγείας.

8. Ομάδα DPIA

- Δρ Μηνάς Κυριακίδης - ΕΑΗΥ
- Έλλη Γιαπάτου Project Manager (ΥΥ)

- Καθ. Παττίχης Κώστας (ΠΚ)
- Φλουρής Ταντελλές (Λειτουργός Ασφάλειας, ΥΥ, ΕΑΗΥ)
- Δρ Μάριος Νεοφύτου (ΠΚ)
- Ειρήνη Γεωργίου DPO, (ΥΥ)
- Ανδρέας Χριστοδούλου DPO, (ΕΑΗΥ)

9. Περιγραφή της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από το NCPeH CY συμπεριλαμβανομένων των ροών δεδομένων

Η αρχιτεκτονική της υποδομής του NCPeH στην Κύπρο περιγράφεται στο Annex TE 1 NCPeH CY Technical deliverable, Section 2.b, όπου δίνεται και το σχηματικό διάγραμμά της. Τα δεδομένα των εγγράφων αποθηκεύονται σε μια κεντρική βάση δεδομένων στο Data Zone. Η περιγραφή του Data Zone δίνεται στο στο Annex TE 1 NCPeH CY Technical deliverable, Section 3.a.v. Επί του παρόντος, η Εθνική Υποδομή Υγειονομικής περίθαλψης βρίσκεται στο Γενικό Νοσοκομείο Αμμοχώστου (ΓΝΑ). Το σύστημα εφαρμόζεται σε περιορισμένο, κλειστό και ασφαλισμένο περιβάλλον όπως αυτό περιγράφεται στο Annex TE 1 NCPeH CY Technical deliverable, Section 3.a.

Λαμβάνοντας υπόψη το σχήμα 1, ένας πάροχος υγειονομικής περίθαλψης μπορεί να έχει πρόσβαση στο σύστημα είτε ως ιατρός του Δημόσιου Τομέα μέσω του Internal Portal Zone που είναι διαθέσιμο μόνο εντός των χώρων των νοσοκομείων μέσω του είτε ως ιατρός ή φαρμακοποιός του Ιδιωτικού Τομέα μέσω του Internet Public Zone όπως περιγράφεται στο Annex TE 1 NCPeH CY Technical deliverable, Section 3.a.i.1 και 3.a.i.2 αντίστοιχα.

Όλοι οι χρήστες πρέπει να είναι πιστοποιημένοι και εξουσιοδοτημένοι από το σύστημα NCP Active Directory (AD) για να έχει πρόσβαση στο σύστημα. Περιγραφή για το NCP AD δίνεται στο Annex TE 1 NCPeH CY Technical Deliverable στα Sections 3.a.ii.2, και 4.a.i και 4.a.ii.

Η υπηρεσία AD είναι μια υπηρεσία καταλόγου που αναπτύχθηκε από την Microsoft για δίκτυα τομέων των Windows. Ένας διακομιστής που εκτελεί υπηρεσίες τομέα Active Directory Domain Services (AD DS) ονομάζεται ελεγκτής τομέα. Η βασική του λειτουργία είναι να εξουσιοδοτεί όλους τους χρήστες και τους υπολογιστές σε έναν τύπο τομέα των Windows που αναθέτει τη δικτύωση και επιβάλλει τις πολιτικές ασφαλείας. Επίσης, το σύστημα χρησιμοποιεί τα τείχη προστασίας, τα οποία είναι συστήματα ασφάλειας δικτύων που παρακολουθούν και ελέγχουν την εισερχόμενη και εξερχόμενη κίνηση του δικτύου βάσει

προκαθορισμένων κανόνων ασφαλείας. Επιπλέον, χρησιμοποιείται και ο μηχανισμός κατά των ιών των ηλεκτρονικών υπολογιστών.

Τέλος, η πλατφόρμα ορίζει και υποστηρίζει διαφορετικούς ρόλους χρηστών. Κάθε ρόλος έχει συγκεκριμένα δικαιώματα πρόσβασης. Για παράδειγμα, ένας γιατρός έχει τη δυνατότητα να προβάλλει και να επεξεργάζεται μόνο ένα αρχείο δεδομένων του ασθενή. Για λόγους ασφαλείας, επιτρέπονται μόνο παρεμβάσεις δεδομένων και καταγράφεται όλη η διαδικασία στο ιστορικό του συστήματος.

Το σύστημα συλλέγει και καταγράφει όλες τις δραστηριότητες κάθε χρήστη σε μια διαφορετική βάση δεδομένων για τη διαχείριση χρηστών. Η διοίκηση και η οργανωτική δομή για την υποστήριξη του Εθνικού συμβουλίου (ΕΣΕΠ) ακολουθούν ένα μοντέλο βέλτιστης πρακτικής που βασίζεται στους κανόνες και τη ρύθμιση και οργάνωση της κυπριακής δημόσιας υπηρεσίας. Δεν υπάρχει πρότυπο ISO. Περισσότερες πληροφορίες δίνονται στο Annex TE 1 NCPeH Technical Deliverable στα Sections 3.a.iii και 4.d.

Οι Λειτουργοί Προστασίας Δεδομένων είναι υπεύθυνοι για περισσότερα από ένα τοπικά σημεία. Η Εθνική Αρχή Ηλεκτρονικής Υγείας έχει υπεύθυνο για τον GDPR (κ Ανδρέα Χριστοδούλου). Το Υπουργείο Υγείας της Κύπρου έχει έναν υπάλληλο που είναι υπεύθυνος για τον GDPR (κα Ειρήνη Γεωργίου). Επίσης, το ΥΥ διαθέτει ένα υπεύθυνο προστασίας δεδομένων και ασφάλειας (κ. Φλουρής Ταντελές) όπου μοιράζεται τα καθήκοντα του και με την Εθνική Αρχή ηλεκτρονικής Υγείας. Είναι ο βασικός υπεύθυνος για το σύστημα διασυνοριακής ανταλλαγής δεδομένων και του τοπικού συστήματος ΟΠΣΝ. Ο κ. Σάββας Ιωάννου εργάζεται στο Τμήμα Υπηρεσιών Πληροφορικής του Υπουργείου Οικονομικών και είναι υπεύθυνος για το Ευρωπαϊκό δίκτυο TESTA.

Σχεδιασμός εφαρμογών: Έχουμε μια Εθνική Πύλη όπου ένας επικυρωμένος Υπεύθυνος Υγείας είναι σε θέση να ολοκληρώσει τα πεδία συμμόρφωσης του epSOS που αντιστοιχούν στην Περίληψη ιστορικού Ασθενών. Ο ασθενής πρέπει να δώσει τη γραπτή συγκατάθεση, η οποία θα φυλάσσεται στον φυσικό ιατρικό φάκελο, πριν τα δεδομένα του αποθηκευτούν στην Εθνική Πύλη. Στη συνέχεια, ο Παροχέας Υγείας είναι σε θέση να πατήσει ένα κουμπί και στη συνέχεια να ανακτήσει την Περίληψη ενός συγκεκριμένου ασθενούς. Η περίληψη ασθενούς δημιουργείται όταν χρειάζεται και όταν ζητείται, λαμβάνοντας υπόψη δεδομένα από τη βάση δεδομένων της Εθνικής Πύλης. Δείτε τα σχετικά διαγράμματα ροής στο Annex TE 1 NCPeH Technical Deliverable στο Section 5.a.

Συλλέγουμε και καταγράφουμε όλες τις δραστηριότητες κάθε χρήστη σε μια διαφορετική βάση δεδομένων για τη διαχείριση χρηστών. Η διοίκηση και η οργανωτική δομή για την υποστήριξη ακολουθούν ένα μοντέλο βέλτιστης πρακτικής που βασίζεται στους κανόνες και τη ρύθμιση και οργάνωση της κυπριακής δημόσιας υπηρεσίας. Δεν υπάρχει πρότυπο ISO.

Β. Αποθήκευση

Τα δεδομένα αποθηκεύονται σε μια κεντρική βάση δεδομένων. Ένας χρήστης πρέπει να έχει πιστοποιηθεί και να έχει εξουσιοδοτηθεί από το ενεργό σύστημα καταλόγου και στη συνέχεια να έχει πρόσβαση στο σύστημα με τους κωδικούς του.

Η Κύπρος ενεργεί ως Εθνικό Σημείο Επαφής NCP-A (ίδια χώρα) και NCP-B (για άλλες χώρες) για Περιλήψεις Ιστορικού Ασθενών. Έτσι, η Κύπρος διαθέτει μια τυποποιημένη λύση λογισμικού - το OpenNCP - που υποστηρίζει τη διασυνοριακή ανταλλαγή δεδομένων προσωπικής υγειονομικής περίθαλψης ως NCP-A, με προδιαγραφές πρωτοκόλλων, διαδικασιών και ανταλλασσόμενων εγγράφων. Συνδέουμε την τεχνική πύλη NCP στην εθνική υποδομή όπως περιγράφεται στο Annex TE 1 NCPeH Technical Deliverable στα Sections 3.a.vii και 4.c.

Το εθνικό δίκτυο ήταν ήδη συνδεδεμένο με το δίκτυο TESTA. Σε Εθνικό επίπεδο έχουν γίνει όλες οι αλλαγές στο τείχος προστασίας για να επιτρέπουν την επισκεψιμότητα από τους διακομιστές του NCP σε συγκεκριμένες διευθύνσεις IP TESTA και σε συγκεκριμένες θύρες. Η κυκλοφορία στο δίκτυο παρακολουθείται από το αρμόδιο τμήμα.

Τέλος, αξίζει να αναφέρουμε ότι δεν υπάρχει διαδικασία για τη διαγραφή οποιουδήποτε εγγράφου. Αποθηκεύουμε όλες τις εκδόσεις της Περίληψης Ασθενών. Τα δεδομένα αποθηκεύονται σε μια κεντρική βάση δεδομένων σε περιορισμένο περιβάλλον σε κυβερνητικές εγκαταστάσεις και δίκτυο.

Γ. Αποθήκευση

Στην πλατφόρμα υπάρχει η διαδικασία συλλογής και καταγραφής της δραστηριότητας κάθε χρήστη, καθώς επίσης και τις εξαιρέσεις αλλά και τα ελαττώματα της. Επίσης υπάρχει ένα σύστημα διαχείρισης χρηστών για ανάκτηση σε περίπτωση ανάλυσης. Το σύστημα χρησιμοποιεί τον εργαλείο OpenSupports όπως αυτό περιγράφεται στο Annex TE 1 NCPeH Technical Deliverable Section 3.a.i.5 και στο Annex OP 9 Service Desk Monitoring Tool.

10. Ταυτοποίηση των κινδύνων

Στόχος αυτού του οδηγού είναι να προσδιοριστούν οι συνθήκες και οι δυνητικοί κίνδυνοι που ενδέχεται να απειλήσουν ή να θέσουν σε κίνδυνο τα προσωπικά δεδομένα του πολίτη / ασθενή και να επηρεάσουν την ιδιωτικότητά του. Η διαδικασία αξιολόγησης του κινδύνου θα εξετάσει κατά κανόνα τους κινδύνους της εφαρμογής NCPeH CY, όσον αφορά την **πιθανότητα εμφάνισής τους** (πιθανότητα) και τον **αντίκτυπο των συνεπειών τους** (σοβαρότητα).

Αυτοί οι κίνδυνοι για την προστασία της ιδιωτικής ζωής συνίστανται κυρίως σε ένα **Feared event** και στις απειλές που μπορεί να προκαλέσουν αυτά τα γεγονότα (πολλές απειλές μπορεί να προκαλέσουν το ίδιο Feared Event).

Τα Feared Events αντιπροσωπεύουν τις ακόλουθες καταστάσεις που πρέπει να αποφεύγονται:

- Παραβιάσεις των νομικών διαδικασιών: δεν υπάρχουν ή δεν υπάρχουν πλέον ή δεν λειτουργούν.
- Αλλαγή της επεξεργασίας: αποκλίνει από αυτό που είχε προγραμματιστεί αρχικά (ένας χρήστης βλέπει πολύ περισσότερα στοιχεία από ότι εξουσιοδοτεί η εργασία του , εκτροπή του σκοπού, υπερβολική ή αθέμιτη προβολή στοιχείων).
- Αθέμιτη πρόσβαση σε προσωπικά δεδομένα: Δεδομένα ασθενών γίνονται γνωστά από μη εξουσιοδοτημένα άτομα.
- Ανεπιθύμητη αλλαγή στα προσωπικά δεδομένα (αλλαγή στοιχείων, διαγνώσεων, φαρμάκων).
- Εξαφάνιση προσωπικών δεδομένων: διαγραφή αρχείων ΗΦΑ, δεν είναι διαθέσιμα ή δεν είναι πλέον διαθέσιμα.
- Εκτροπή των προσωπικών δεδομένων σε άλλους χρήστες: αποστολή στοιχείων σε μη εξουσιοδοτημένους χρήστες, διανέμονται σε άτομα που δεν χρειάζονται.

Κάθε φορά που θα συμβούν αυτά τα γεγονότα, θα έχουν επιπτώσεις στην ιδιωτική ζωή των υποκειμένων των δεδομένων και οι εν λόγω επιπτώσεις θα πρέπει να αξιολογούνται σωστά και συστηματικά και τελικά να μετριάζονται.

Τυχαία ή σκόπιμα, αυτά τα Feared Events θα ενεργοποιηθούν από μία ή περισσότερες πηγές κινδύνου, κυρίως τις εξής:

- Πρόσωπα εντός του οργανισμού: τα άτομα που ανήκουν στον οργανισμό: χρήστης, διαχειριστής συστήματος, διαχειριστής δικτύου, φορέας εκμετάλλευσης υπηρεσιών, Λειτουργός της ΕΑΗΥ, Λειτουργός του ΥΥ ή των Ι.Υ,

- Εξωτερικοί συνεργάτες: άτομα εκτός του οργανισμού: αποδέκτης, πάροχος, ανταγωνιστής, εξουσιοδοτημένος τρίτος, κυβερνητικός οργανισμός, ανθρώπινη δραστηριότητα που περιβάλλει, εξωτερική / υπεργολαβική συντήρηση
- Μηχανή: μη ανθρώπινες πηγές: ιός υπολογιστών, φυσική καταστροφή όπως κεραυνός, ενεργειακή ανισορροπία, διακοπή ενέργειας και διακοπή λειτουργίας.

11. Ταυτοποίηση/ανάλυση ρίσκων/απειλών

Προκειμένου να διευκολυνθεί ο προσδιορισμός των απειλών, παρέχεται παρακάτω ένας μη εξαντλητικός κατάλογος γενικών απειλών. Ο κατάλογος αυτός συζητήθηκε και σχολιάστηκε από την επιτροπή ασθενών και τον υπεύθυνο προστασίας δεδομένων DPO του νοσοκομείου, το Διοικητικό συμβούλιου της ΕΑΗΥ, διευθυντή ΓΝΑ, Διευθυντή έργου, τον υπεύθυνο της αρχής Η.Υ, τον υπεύθυνο χρηστών και την ομάδα του έργου. Προσδιορίστηκε επίσης αριθμός controls που μπορούν να εφαρμοστούν ή να ενισχυθούν, καθώς και το επίπεδο του Ρίσκου.

Οι γενικές απειλές ομαδοποιούνται ανάλογα με τον αντίκτυπό τους στην:

i. εμπιστευτικότητα,
ii. την ακεραιότητα και τη
iii. διαθεσιμότητα των δεδομένων
iv. Άλλες Γενικές απειλές

11.1 Απειλές που μπορεί να θέσουν σε κίνδυνο την εμπιστευτικότητα

Ο παρακάτω πίνακας παρουσιάζει τις γενικές απειλές που μπορούν να οδηγήσουν σε (feared events):

- Παράνομη πρόσβαση σε προσωπικά δεδομένα,
- Η ανεπιθύμητη αλλαγή των προσωπικών δεδομένων
- Απώλεια προσωπικών Δεδομένων

Γενικές Απειλές	Επεξήγηση	Παραδείγματα	Οδηγίες /Υποδείξεις	Controls
Μη ασφαλής φυσιολογική Χρήση υλισμικού.	τη χρήση ή τη μεταφορά ευαίσθητου υλικού για προσωπικούς σκοπούς κ.λπ..	Η χρήση μη ελεγχόμενου υλικού μπορεί να εισάγει ιούς σε ένα κανονικά καθαρό περιβάλλον. Οι εταιρείες που πιστεύουν ότι είναι ασφαλείς έναντι των απειλών στο Internet καθίστανται ευάλωτες σε απροσδόκητο κακόβουλο λογισμικό	Λήψη μέτρων προστασίας από ιούς και κακόβουλα προγράμματα σε όλα τα σημεία Προστασία από τη χρήση άγνωστων συσκευών αποθήκευσης (π.χ. συσκευές USB);	Μείωση ευπάθειας λογισμικού Μείωση των τρωτών σημείων των δικτύων επικοινωνιών υπολογιστών

Κατασκοπία εκ του σύνεγγυς και μακρόθεν	Παρακολουθώντας την οθόνη ενός ατόμου χωρίς να γνωρίζει κανείς κατά τη διάρκεια της εργασίας. λήψη φωτογραφίας οθόνης. γεωγραφική θέση του υλικού την απομακρυσμένη ανίχνευση των ηλεκτρομαγνητικών σημάτων κλπ.	Όπου οι καλωδιώσεις χαλκού εξακολουθούν να χρησιμοποιούνται. Αυτό καθιστά δυνατή την ερμηνεία και την επαναχρησιμοποίηση των σημάτων που στέλνονται μέσω του δικτύου επικοινωνιών.	αντικατάσταση το μέρος του χαλκού με ίνες Χρησιμοποιούνται προστατευτικά οθόνης για να καταστεί αδύνατη η θέαση στην οθόνη ή η λήψη φωτογραφιών της οθόνης; έλεγχοι απομακρυσμένης πρόσβασης σε μια μη προστατευμένη περιοχή (π.χ. WiFi, Bluetooth, υπέρυθρες);	Μείωση ευπάθειας υλικού

Απώλεια Υλισμικού	Κλοπή φορητού υπολογιστή από δωμάτιο ξενοδοχείου. κλοπή επαγγελματικού κινητού τηλεφώνου ι. ανάκτηση μιας απορριπτόμενης συσκευής ή υλικού αποθήκευσης. απώλεια ηλεκτρονικής συσκευής αποθήκευσης κ.λπ.	Κάθε συσκευή που περιέχει ευαίσθητα δεδομένα σχετικά με το περιβάλλον θα προκαλέσει απαράδεκτο κίνδυνο αλλαγής και κατάχρησης αυτών των δεδομένων. Όταν ανακτώνται πληροφορίες σχετικά με το εμπορικό σήμα και τον τύπο των τείχους προστασίας, το εύρος IP, το σύμβολο και τον τύπο του συστήματος και του SCADA, μια σοβαρή επίθεση καθίσταται εύκολη.	κωδικός πρόσβασης, κωδικός PIN, βιομετρική αναγνώριση, αναγνώριση προτύπου) κρυπτογραφημένα τα δεδομένα στο υλικό;	Μείωση ευπάθειας υλικού Μείωση των τρωτών σημείων που σχετίζονται με την κυκλοφορία εγγράφων σε χαρτί

Προβολή εγγράφων σε χαρτί	Ανάγνωση, φωτοτυπία, φωτογράφηση κλπ.	Χαρτί έγγραφα με προσωπική (μέτρηση, τιμολόγηση) οι πληροφορίες των καταναλωτών δεν αποθηκεύονται με ασφάλεια και επομένως είναι προσιτές σε μη εξουσιοδοτημένα άτομα.	1. Λαμβάνονται μέτρα για την αποφυγή μη εξουσιοδοτημένης πρόσβασης σε έγγραφα σε χαρτί με προσωπικά δεδομένα; 2. Είναι εγκατεστημένη η εκτύπωση κατά παραγγελία; 3. Υπάρχουν διαθέσιμα ασφαλή ντουλάπια για την αποθήκευση τυπωμένων δεδομένων;	Μείωση των τρωτών σημείων του τα άτομα Μείωση των τρωτών σημείων του χαρτί έγγραφα Μείωση των τρωτών σημείων που σχετίζονται με την κυκλοφορία εγγράφων σε χαρτί
Απομακρυσμένη απώλεια πληροφοριών	Μη ακούσια αποκάλυψη πληροφοριών ενώ μιλάτε. χρήση συσκευών ακρόασης για να παρακολουθήσετε συναντήσεις κ.λπ.	Λειτουργοί που μιλάνε για προσωπικές πληροφορίες από τους καταναλωτές στις συναντήσεις τους ή τους κοινόχρηστους χώρους.	1. Είναι ενημερωμένοι οι εργαζόμενοι σχετικά με την ασφάλεια, τους κινδύνους ασφάλειας και τα τρωτά σημεία; 2. Είναι μέρος της συνειδητοποίησης των συναντήσεων εργασίας 3. Είναι κοινά τα περιστατικά να μαθαίνουν από αυτά;	Μείωση των τρωτών σημείων των ατόμων

Λογισμικό Keylogger / Trojan Horse	Software Key-logger καταγράφει όλες τις πληκτρολογήσεις και / ή το Trojan στέλνει εντολές και δεδομένα στον υπολογιστή του εισβολέα Σύστημα	Επιτρέπει στους εισβολείς να σχεδιάζουν και να επαναχρησιμοποιούν ονόματα χρηστών, κωδικούς πρόσβασης, συμβιβασμούς δεδομένων που πρέπει να τηρούνται και να αναζητούν συγκεκριμένες λέξεις, προτάσεις κλπ.	1. Είναι όλα τα συστήματα υπολογιστών εξοπλισμένα με λύσεις κατά των ιών, αντιμολικών; (εάν είναι διαθέσιμο για το συγκεκριμένο λειτουργικό σύστημα) 2. Ενημερώνονται καθημερινά οι λύσεις κατά του κακόβουλου λογισμικού και των ιών; 3. Είναι ο ιός anti-virus ρυθμισμένος έτσι ώστε ο πλήρης υπολογιστή να σαρώνει σε τακτική βάση;	Μείωση ευπάθειας λογισμικού

11.2 Απειλές που μπορεί να θέσουν σε κίνδυνο την ακεραιότητα

Feared Events

1. Παράνομη πρόσβαση σε προσωπικά δεδομένα,
2. Η ανεπιθύμητη αλλαγή των προσωπικών δεδομένων
3. Απώλεια προσωπικών Δεδομένων

Γενικές Απειλές	Επεξήγηση	Παραδείγματα	Οδηγίες	Controls
μεταβολές στο λογισμικό	Σφάλματα κατά τη διάρκεια ενημερώσεων, διαμόρφωσης ή συντήρησης. λοίμωξη από κακόβουλο κώδικα. αντικατάσταση εξαρτημάτων κ.λπ..	Η αλλαγή λογισμικού μπορεί να οδηγήσει σε αλλαγές δεδομένων που θα βλάψουν την ακεραιότητα του ep & Ps. Αυτό μπορεί να επηρεάσει το προφίλ υγείας και τη συνταγή.	Να Εξετάζονται οι ενημερώσεις λογισμικού σε δοκιμαστικό περιβάλλον, πριν από τη χρήση τους στο επιχειρησιακό περιβάλλον. Να Εξετάζονται οι κώδικες πηγής, όταν το λογισμικό είναι προσαρμοσμένο ή προσαρμοσμένο για ένα συγκεκριμένο σύστημα.	Μείωση ευπάθειας λογισμικού

Ανεπαρκής μηχανισμός καταγραφή logging mechanism	Δεν καταγράφει τις διοικητικές διαδικασίες.	After an incident, or just for routine checks, είναι απαραίτητο να έχουμε πληροφορίες καταγραφής (logs) για να επεξηγήσουμε προηγούμενες δραστηριότητες.	έλεγχοι ασφαλείας καταγραφή της πρόσβασης στα προσωπικά δεδομένα	Παρακολούθηση έλεγχοι πρόσβασης Διαχείριση παραβιάσεων προσωπικών δεδομένων Παρακολούθηση της δραστηριότητας στα IT Συστήματα

Ελλιπείς πληροφορίες	Οι πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων σχετικά με το σκοπό και τη χρήση των δεδομένων δεν είναι πλήρεις	Οι πληροφορίες που παρέχονται στους καταναλωτές είναι ανεπαρκείς	Να γνωστοποιήσατε στον καταναλωτή τον σκοπό της επεξεργασίας των προσωπικών δεδομένων.	Ενημέρωση των υποκειμένων των δεδομένων Σαφής και συνεπής επικοινωνία του σκοπού και των στόχων της συλλογής δεδομένων

Πρόληψη των ενστάσεων	Τα υποκείμενα δεδομένων έχουν το δικαίωμα να αντιταχθούν στην επεξεργασία δεδομένων. Εάν θέλουν να εκτελέσουν αυτό το δικαίωμα, πρέπει να είναι (τεχνικά) δυνατό.	Ασθενής αρνείται τη συμπερίληψη στοιχείων του στον ΗΦΑ	Να Είναι δυνατή η αλλαγή της συλλογής δεδομένων προσωπικού χαρακτήρα μετά την αντίρρηση του καταναλωτή. Να Μπορούν οι καταναλωτές να αντιταχθούν στην επεξεργασία των προσωπικών δεδομένων.	Επιτρέποντας την άσκηση του δικαίωμα να αντιταχθεί Ελαχιστοποίηση του αριθμού των προσωπικών δεδομένων Διαχείριση περιόδων αποθήκευσης προσωπικών δεδομένων Ενημέρωση των υποκειμένων των δεδομένων Λήψη της συγκατάθεσης των υποκειμένων των δεδομένων

Ασαφείς αρμοδιότητες για την επεξεργασία δεδομένων.	Δεν είναι σαφές στα υποκείμενα των δεδομένων ποια είναι τα μέρη που εμπλέκονται στην επεξεργασία των δεδομένων και τους αντίστοιχους ρόλους τους.	(1) Ο οργανισμός εγκατάστασης ενεργεί ως υπεργολάβος	Οι ευθύνες να περιγράφονται σαφώς και να πραγματοποιούνται για όλα τα μέρη Η επεξεργασία δεδομένων μέρος της σύμβασης υπεργολάβου.	Ενημέρωση των υποκειμένων των δεδομένων Δημιουργήστε μια πολιτική απορρήτου, έναν κώδικα δεοντολογίας ή βεβαιώστε ότι η επεξεργασία των δεδομένων είναι πιο διαφανής

Έλλειψη πρόσβασης σε προσωπικά δεδομένα	Δεν υπάρχει τρόπος για το υποκείμενο των δεδομένων να προβεί σε διόρθωση ή διαγραφή των δεδομένων του. Ο υπεύθυνος επεξεργασίας ή / και ο επεξεργαστής δεν είναι επαρκώς προετοιμασμένοι για να ανταποκριθούν σε τέτοιου είδους αιτήματα.	Δεν είναι δυνατή η δημιουργία εξατομικευμένης επισκόπησης των προσωπικών δεδομένων από τη βάση δεδομένων που περιέχει τα δεδομένα.	Να Υπάρχουν διαδικασίες για την ικανοποίηση των δικαιωμάτων του καταναλωτή όσον αφορά τη συλλογή, την πρόσβαση, τη διαγραφή και τη διόρθωση δεδομένων. να δώσετε μια επισκόπηση των στοιχείων που συλλέξατε. Να Είστε σε θέση να παράσχετε ποια δεδομένα μεταφέρονται σε τρίτους. να Μπορείτε διαγράψετε τα δεδομένα κατόπιν αιτήματος.	Επιτρέποντας την άσκηση του δικαίωμα άμεσης πρόσβασης Επιτρέποντας την άσκηση του δικαιώματος να διορθώσετε Σχεδιασμός, υλοποίηση και διάθεση ενός συστήματος αντιμετώπισης των καταγγελιών, που υποστηρίζεται από σοβαρές κυρώσεις και επιβολή εξουσίες Δώστε τον επιμέρους έλεγχο στα δεδομένα του, για παράδειγμα μέσω μιας ασφαλούς δικτυακής πύλης

Αδυναμία απάντησης σε αιτήματα πρόσβασης, διόρθωσης ή διαγραφής δεδομένων, με έγκαιρο και ικανοποιητικό τρόπο.	Τα δεδομένα διανέμονται σε διάφορες επιχειρηματικές μονάδες και μια ολοκληρωμένη επισκόπηση δεν μπορεί να γίνει σε σύντομο χρονικό διάστημα.	Ο συνδυασμός αυτών των δεδομένων από διαφορετικά συστήματα σε μια επισκόπηση απαιτεί (πολύ) προσπάθεια.	να δώσετε μια επισκόπηση των στοιχείων που συλλέξατε. να παράσχετε ποια δεδομένα μεταφέρονται σε τρίτους να γίνει μια επισκόπηση των στοιχείων που παρέχονται σε ποιον πρέπει να παρέχονται. να Μπορείτε διαγράψετε τα δεδομένα κατόπιν αιτήματος.	Επιτρέποντας την άσκηση του δικαίωμα να διορθώσετε Σχεδιασμός, υλοποίηση και διάθεση ενός συστήματος ανταπόκριση και αντιμετώπιση παραπόνων, το οποίο υποστηρίζεται από σοβαρές κυρώσεις και επιβολή εξουσίες Δώστε τον επιμέρους έλεγχο στα δεδομένα του, για παράδειγμα μέσω μιας ασφαλούς δικτυακής πύλης

11.3 Απειλές που μπορεί να θέσουν σε κίνδυνο τη διαθεσιμότητα

Feared events

1. Η ανεπιθύμητη αλλαγή των προσωπικών δεδομένων
2. Απώλεια προσωπικών Δεδομένων

Γενικές Απειλές	Επεξήγηση	Παραδείγματα	Οδηγίες	Controls
Απώλεια Υλισμικού	Κλοπή φορητού υπολογιστή από δωμάτιο ξενοδοχείου. κλοπή επαγγελματικού κινητού τηλεφώνου από πορτοφόλι. ανάκτηση μιας απορριπτόμενης συσκευής ή υλικού αποθήκευσης. απώλεια ηλεκτρονικής συσκευής αποθήκευσης κ.λπ.	Κάθε συσκευή που περιέχει ευαίσθητα δεδομένα σχετικά με το περιβάλλον Θα προκαλέσει απαράδεκτο κίνδυνο αλλαγής και κατάχρησης αυτών των δεδομένων. Όταν ανακτώνται πληροφορίες σχετικά με το εμπορικό σήμα και τον τύπο των τείχους προστασίας, το εύρος IP, το σύμβολο και τον τύπο του συστήματος και του SCADA, μια σοβαρή επίθεση καθίσταται εύκολη.	οι συσκευές που περιέχουν δεδομένα που να προστατεύονται από κατάχρηση (κωδικός πρόσβασης, κωδικός PIN, βιομετρική αναγνώριση, αναγνώριση προτύπου) κρυπτογραφημένα τα δεδομένα.	Μείωση ευπάθειας υλικού Μείωση των τρωτών σημείων που σχετίζονται με την κυκλοφορία εγγράφων σε χαρτί

Απώλεια ισχύος (ηλεκτρισμού)	Η απώλεια ισχύος μπορεί να βλάψει το υλικό και το λογισμικό και να οδηγήσει στη μη διαθεσιμότητα των υπολογιστικών συστημάτων, του εξοπλισμού δικτύου και της διακοπής των συσκευών έξυπνων δικτύων	Παραδείγματα: Λόγω της απώλειας ισχύος των σκληρών δίσκων ή άλλων εξαρτημάτων υλικού. Λόγω της απώλειας ισχύος του λειτουργικού συστήματος ή της απώλειας μη αποθηκευμένων δεδομένων. Η μεγάλη απώλεια ισχύος επηρεάζει τη διαθεσιμότητα των συστημάτων. Δεν θα καλύπτονται όλα τα συστήματα από εξοπλισμό ηλεκτρικής ενέργειας έκτακτης ανάγκης. Πολύ μεγάλη απώλεια ισχύος θα οδηγήσει σε διακοπή της παροχής ενέργειας έκτακτης ανάγκης και έλλειψη ενέργειας έκτακτης ανάγκης.	UPS	Μείωση των τρωτών σημείων του λογισμικού Μείωση των τρωτών σημείων του λογισμικού Μείωση των τρωτών σημείων του of computer communications networks

11.4 Άλλες γενικές απειλές που ενδέχεται να θέσουν σε κίνδυνο τα προσωπικά δεδομένα

Feared Events

1. Παραβιάσεις των νομικών διαδικασιών,
2. Η ανεπιθύμητη αλλαγή των προσωπικών δεδομένων
3. Αλλαγές στην επεξεργασία

Γενικές Απειλές	Επεξήγηση	Παραδείγματα	Οδηγίες	Controls
Υπερβάσεις συλλογής δεδομένων	Συλλέγονται περισσότερα προσωπικά δεδομένα από αυτά που είναι απαραίτητα για την επίτευξη συγκεκριμένου σκοπού.	Συλλογή λεπτομερέστερων δεδομένων προφίλ φορτίου για τον σκοπό αυτό, όπου πολύ λιγότερο λεπτομερή δεδομένα θα ήταν επαρκή για την επίτευξη του ίδιου στόχου.	Τα δεδομένα που συλλέγονται ανάλογα με το σκοπό	Ελαχιστοποίηση του ποσού προσωπικά δεδομένα Ενεργός μέτρο για την παρεμπόδιση της χρήσης συγκεκριμένων δεδομένων Περιορισμοί στη χρήση πληροφοριών για πολύ συγκεκριμένο σκοπό, με ισχυρές νομικές, οργανωτικές και τεχνικές εγγυήσεις που εμποδίζουν την εφαρμογή

				τους για οποιονδήποτε άλλο σκοπό Ελαχιστοποίηση του αριθμού των προσωπικών δεδομένων Διαχείριση περιόδων πρόσβασης / αποθήκευσης προσωπικών δεδομένων Ενημέρωση των υποκειμένων των δεδομένων Λήψη της συγκατάθεσης των υποκειμένων των δεδομένων

Γενικές Απειλές	Επεξήγηση	Παραδείγματα	Οδηγίες	Controls

Μη αδειοδοτημένη συλλογή.	Κάποια δεδομένα καταγράφονται κρυφά και ως εκ τούτου άγνωστα στο υποκείμενο των δεδομένων.	πραγματοποιούνται καταγραφές από άλλα συστήματα χωρίς την ευαισθητοποίηση του καταναλωτή.	Ενημερώνονται οι Ασθενείς για τη συλλογή προσωπικών δεδομένων, το χρονοδιάγραμμα, τη διατήρηση δεδομένων, τη χρήση τους	Ενημέρωση των υποκειμένων των δεδομένων Σαφής και συνεπής επικοινωνία του σκοπού και των στόχων της συλλογής δεδομένων

Παραβίαση της ρητής συναίνεσης	Όταν η συναίνεση χρησιμοποιείται ως νομική βάση για την επεξεργασία δεδομένων, πρέπει να είναι: (α) ελεύθερα β) ειδικά και (γ) ενημερωμένη ένδειξη των επιθυμιών του χρήστη. Εάν κάποια από αυτές τις προϋποθέσεις δεν πληρούνται, η συγκατάθεση είναι άκυρη.	(1) ο καταναλωτής δεν ενημερώνεται για το ενδεχόμενο να αποκαλυφθούν τα δεδομένα του προφίλ του φορτίου σε τρίτους για εμπορία (4) ο καταναλωτής παρέχει τη συγκατάθεση βάσει των γενικών όρων της σύμβασης (5) Οι καταναλωτές αποδέχονται καθεστώς χωρίς υπογραφή.	ζητήσατε και λάβετε τη ρητή συγκατάθεση. συνέπειες εάν δεν δοθεί η συναίνεσή του	Ενημέρωση των υποκειμένων των δεδομένων Λήψη δεδομένων συγκατάθεση των υποκειμένων Μη είσπραξη αμφισβητούμενων δεδομένων Μη συλλογή αναγνωρίσιμων πληροφοριών, μόνο ψευδώνυμα, ή ανώνυμα δεδομένα Χρήση μαθηματικών μεθόδων χωρίς συλλογή και εγγραφή δεδομένων προέλευσης σε επίτευξη στόχων Σαφής και συνεπής επικοινωνία του σκοπού και

				των στόχων της συλλογής δεδομένων

Μη νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα	Η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν βασίζεται σε συγκατάθεση, σύμβαση, νομική υποχρέωση ή άλλη σχετική νομική βάση σύμφωνα με το άρθρο 7 της οδηγίας 95/46 / ΕΚ.	1) Ο λειτουργός μοιράζεται τις πληροφορίες που έχει συλλέξει με τρίτους χωρίς προειδοποίηση, συγκατάθεση ή όπως άλλως νομιμοποιείται. (2) Τα νέα μέρη συνδέουν και χρησιμοποιούν πληροφορίες για σκοπούς που δεν προβλέπονται από το νόμο.	συλλογή προσωπικών δεδομένων βασισμένη σε ρητή συγκατάθεση ή / και νόμιμους λόγους. ο νόμιμος λόγος συλλογής των προσωπικών δεδομένων	Λήψη της συγκατάθεσης των υποκειμένων των δεδομένων Ελαχιστοποίηση του ποσού προσωπικά δεδομένα Δημιουργήστε μια πολιτική απορρήτου, έναν κώδικα δεοντολογίας ή βεβαιώστε ότι η επεξεργασία των δεδομένων είναι πιο διαφανής

11.5 Ανάλυση Ρίσκου

Επίπεδο	Σοβαρότητα / επιπτώσεις
< 5	1. Αμελητέα
= 5	2. Περιορισμένη
= 6	3. Σημαντική
> 6	4. Μέγιστη

Υποστήριξη + πηγή κινδύνου	Πιθανότητα να συμβεί
< 5	1. Αμελητέα
= 5	2. Περιορισμένη
= 6	3. Σημαντική
> 6	4. Μέγιστη

Feared events		**Αντίκτυπος**	**Πιθανότητα**	**Επίπεδο Ρίσκου**
1. Απώλεια Δεδομένων		4	2	6= Σημαντικό
2 Η ανεπιθύμητη αλλαγή των δεδομένων		4	1	5= Περιορισμένη
3. Παράνομη πρόσβαση σε δεδομένα,		4	1	5= Περιορισμένη
4. Παραβιάσεις των νομικών διαδικασιών		3	2	5= Περιορισμένη
5. Αλλαγές στην επεξεργασία		4	2	6= Σημαντικό

Feared events		**Controls**
1. Απώλεια Δεδομένων		Λήψη μέτρων προστασίας από ιούς και κακόβουλα προγράμματα σε όλα τα σημεία Προστασία από τη χρήση άγνωστων συσκευών αποθήκευσης Μείωση της διαθεσιμότητας του PS&eP
2 Η ανεπιθύμητη αλλαγή των δεδομένων		Λήψη μέτρων προστασίας από ιούς και κακόβουλα προγράμματα σε όλα τα σημεία Προστασία από τη χρήση άγνωστων συσκευών αποθήκευσης. Ελαχιστοποίηση του ποσοστού πρόσβασης σε προσωπικά δεδομένα
3. Παράνομη πρόσβαση σε δεδομένα,		Προστασία από τη χρήση άγνωστων συσκευών αποθήκευσης Μη συλλογή αναγνωρίσιμων πληροφοριών, μόνο ψευδώνυμα, ή ανώνυμα δεδομένα. Διαχείριση περιόδων πρόσβασης προσωπικών δεδομένων
4. Παραβιάσεις των νομικών διαδικασιών		Ελαχιστοποίηση του ποσοστού πρόσβασης σε προσωπικά δεδομένα Ενεργό μέτρο για την παρεμπόδιση της χρήσης συγκεκριμένων δεδομένων κατά τη λήψη αποφάσεων Περιορισμοί στη χρήση πληροφοριών για πολύ συγκεκριμένο σκοπό, με ισχυρές νομικές, οργανωτικές και τεχνικές εγγυήσεις που εμποδίζουν την εφαρμογή τους για οποιονδήποτε άλλο σκοπό Ελαχιστοποίηση του αριθμού των προσωπικών δεδομένων Ενημέρωση/Συγκατάθεση Σαφής και συνεπής επικοινωνία του σκοπού και των στόχων της συλλογής δεδομένων
5. Αλλαγές στην επεξεργασία		Ενημέρωση των υποκειμένων των δεδομένων Λήψη της συγκατάθεσης των υποκειμένων των δεδομένων Σαφής και συνεπής επικοινωνία του σκοπού και των στόχων της συλλογής δεδομένων

Παράρτημα Ι

Νομικές Διαδικασίες (Controls)

Καθορισμένο, ρητό και νόμιμο σκοπό.	Καθορίζεται
Περιορισμό του αριθμού των προσωπικών δεδομένων.	Τα δεδομένα καθαρίζονται από το έργο
Περίοδος που απαιτείται για την επίτευξη των σκοπών, ελλείψει άλλης νομικής υποχρέωσης που επιβάλλει μεγαλύτερη περίοδο διατήρησης	Η περίοδος δεν καθορίζεται ούτε περιορίζεται (pending)
Σεβασμός του δικαιώματος ενημέρωσης των υποκειμένων των δεδομένων.	Ενημερώνονται
Διατήρηση της ποιότητας των προσωπικών δεδομένων.	Ελέγχεται περιοδικά (σχεδιάζεται)
Σεβασμός του δικαιώματος των προσώπων να έχουν πρόσβαση τα δεδομένα τους.	Σχεδιάζεται
Λήψη της συγκατάθεσης των υποκειμένων των δεδομένων ή ύπαρξη άλλου νομικού	Ναι
Σεβασμό του δικαιώματος άρνησης των υποκειμένων των δεδομένων.	Ναι
Σεβασμός του δικαιώματος των προσώπων στα οποία αναφέρονται τα δεδομένα να διορθώνουν τα δεδομένα τους και	Ναι μετά από επίσκεψη

Έλεγχοι αντιμετώπισης κινδύνου

Επιλεγμένα στοιχεία ελέγχου (υπάρχοντα ή προγραμματισμένα):

1. Οργανωτικοί έλεγχοι: οργάνωση, πολιτική, διαχείριση κινδύνου, έργο

διαχείριση, διαχείριση συμβάντων, επίβλεψη κλπ.

2. Λογικοί έλεγχοι ασφαλείας: ανώνυμο, κρυπτογράφηση, δημιουργία αντιγράφων ασφαλείας, λογικός έλεγχος πρόσβασης κ.λπ.

3. Έλεγχοι φυσικής ασφάλειας: φυσικός έλεγχος πρόσβασης, ασφάλεια υλικού.

Εθνική Αρχή Ηλεκτρονικής Υγείας

Ανδρέας Χριστοδούλου

Υπεύθυνος DPO

Γωνία Προδρόμου 1 & Χείλωνος 17

1448 Λευκωσία, Κύπρος

Τηλεφωνικό Κέντρο: 00357 22 605 300/301

Υπουργείο Υγείας

Ειρήνη Γεωργίου

Υπεύθυνη DPO

Γωνία Προδρόμου 1 & Χείλωνος 17

1448 Λευκωσία, Κύπρος

Τηλεφωνικό Κέντρο: 00357 22 605 300/301