ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 14-07-2015

Αριθ. Πρωτ.: Γ/ΕΞ/3928/14-07-2015

Γ Ν Ω Μ Ο Δ Ο Τ Η Σ Η 2/2015

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε μετά από πρόσκληση του Προέδρου της σε συνεδρίαση την 17-3-2015 στην έδρα της, σε συνέχεια της από 30-7-2014 συνεδρίασης και εξ αναβολής της από 23-7-2014, 17-2-2015 και 3-3-2015 συνεδρίασής της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας.

Παρέστησαν ο Πρόεδρος Π. Χριστόφορος και τα τακτικά μέλη της Αρχής Λ. Κοτσαλής, Α.–Ι. Μεταξάς, Δ. Μπριόλας, Α. Συμβώνης, Κ. Χριστοδούλου, Π. Τσαντίλας, ως εισηγητής καθώς και το αναπληρωματικό μέλος της Αρχής Π. Ροντογιάννης, επίσης ως εισηγητής. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν επίσης, με εντολή του Προέδρου, οι Χ. Λάτσιου, Γ. Παναγοπούλου, ειδικοί επιστήμονες – ελέγκτριες, και ο Φ. Μίτλεττον, ειδικός επιστήμονας – ελεγκτής, ως βοηθοί εισηγητή. Ως βοηθός εισηγητή είχε οριστεί η Ζωή Καρδασιάδου, ειδική επιστήμονας – ελέγκτρια, η οποία λόγω κωλύματος δεν παρέστη στις συνεδριάσεις της 17-2-2015, 3-3-2015 και 17-3-2015. Παρέστη, επίσης, με εντολή του Προέδρου, η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας,.

Η Αρχή συνεδρίασε προκειμένου να γνωμοδοτήσει, σύμφωνα με το άρθρο 19 παρ. 1 στοιχ. θ΄ του ν. 2472/1997, επί ερωτήματος της 7^{η} Υγειονομικής Περιφέρειας (ΥΠΕ) Κρήτης σχετικά με τη λειτουργία συστήματος ηλεκτρονικού ιατρικού φακέλου, με την επωνυμία «ΠΑΝΑΚΕΙΑ», στο πλαίσιο του Ολοκληρωμένου Πληροφοριακού

Συστήματος Υγείας (ΟΠΣΥ) Κρήτης. Η 7η ΥΠΕ Κρήτης με το με αρ. πρωτ. …/…-…-…-έγγραφό της (αρ. πρωτ. Αρχής Γ/ΕΙΣ/2387/3-4-2013) έθεσε στην Αρχή ερωτήματα σχετικά με τη λειτουργία συστήματος ηλεκτρονικού ιατρικού φακέλου στο πλαίσιο του ΟΠΣΥ Κρήτης. Η Αρχή στη συνέχεια κάλεσε με το με αρ. πρωτ. Γ/ΕΞ/4613/23-7-2014 έγγραφο την 7η ΥΠΕ Κρήτης στη συνεδρίαση της 30-7-2014, η οποία παρέστη δια των εκπροσώπων της Άννας Τριχοπούλου, νόμιμης εκπροσώπου, Β, Δ/ντή Πληροφορικής και Γ Νευροχειρουργού, ο οποίος ανήκει στην ομάδα που επεξεργάζεται το σύστημα «ΠΑΝΑΚΕΙΑ».

Η 7η ΥΠΕ Κρήτης έλαβε προθεσμία και κατέθεσε το με αρ. πρωτ. Γ/ΕΙΣ/5109/27-8-2014 υπόμνημα. Με το υπόμνημα αυτό η 7η ΥΠΕ Κρήτης ενημερώνει την Αρχή σχετικά με τη λειτουργία του συστήματος «ΠΑΝΑΚΕΙΑ», την αρχιτεκτονική, τα μέτρα ασφάλειας, τον τρόπο λήψης συγκατάθεσης από τον ασθενή καθώς και τη διαδικασία πρόσβασης στα δεδομένα που τηρούνται στο σύστημα. Επαναδιατυπώνει επίσης ερωτήματα τα οποία είχε θέσει και στο αρχικό με αρ. πρωτ. …/…-…-… έγγραφό της (αρ. πρωτ. Αρχής Γ/ΕΙΣ/2387/3-4-2013).

Τα ερωτήματα αφορούν στην δυνατότητα επισκόπησης παρελθόντων περιστατικών νοσηλείας του ασθενούς από άλλες κλινικές και την ανάγκη συγκατάθεσης του ασθενούς για την πρόσβαση του θεράποντος ιατρού στα στοιχεία του συστήματος. Επίσης τίθεται το ερώτημα αν ο ασθενής δεν έχει την ικανότητα δικαιοπραξίας, ποιος νομιμοποιείται να δώσει την έγκριση ή μη της πρόσβασης στον ιατρικό φάκελο ασθενούς καθώς και ποιος έχει νόμιμο δικαίωμα πρόσβασης και με ποια διαδικασία στον ιατρικό φάκελο ασθενούς. Επίσης ερωτάται η Αρχή σχετικά με το πώς μπορεί ο ασθενής να λάβει όλο τον φάκελο υγείας του που έχει καταγραφεί στις Μονάδες Υγείας καθώς επίσης και το ζήτημα του χρόνου τήρησης των ιατρικών δεδομένων του συστήματος. Ζητείται τέλος η αποστολή παρατηρήσεων/προσαρμογών που πρέπει να γίνουν, ώστε να υπάρχει συμμόρφωση με τις απαιτήσεις της Αρχής.

Όπως περιγράφεται στο υπόμνημα, «*… το εν λόγω σύστημα αποτελεί σύστημα διαχείρισης των πληροφοριών κατά τη νοσηλεία του ασθενούς, προσφέροντας στον επαγγελματία υγείας τη σωστή πληροφορία τη στιγμή που τη χρειάζεται, με ένα τρόπο που να μπορεί εύκολα να εποπτεύσει το περιστατικό νοσηλείας*.».

Σύμφωνα με το σύστημα ΠΑΝΑΚΕΙΑ όπως έχει σχεδιαστεί, ο ιατρός διαθέτει άμεσα, για τον ασθενή που νοσηλεύει, μέσω του συστήματος, ιστορικά στοιχεία νοσηλείας από νοσηλείες σε Μονάδες Υγείας της 7ης ΥΠΕ, καθώς και στοιχεία της παρούσας νοσηλείας.

Η αρχιτεκτονική του συστήματος ΠΑΝΑΚΕΙΑ περιλαμβάνει τον διακομιστή βάσης δεδομένων (database server), τον διακομιστή εφαρμογών (application server), τον διακομιστή επικοινωνίας (communication server) της 7ης ΥΠΕ. Υπάρχουν τρία ασφαλή και κρυπτογραφημένα κανάλια επικοινωνίας με τον «έξω κόσμο»: επικοινωνία του διακομιστή βάσης δεδομένων (database server) της 7ης ΥΠΕ με τον εφεδρικό διακομιστή (backup server) που βρίσκεται σε κάποια Μονάδα Υγείας, επικοινωνία μεταξύ του διακομιστή εφαρμογών (application server) της 7ης ΥΠΕ με τους χρήστες των Μονάδων Υγείας, επικοινωνία των διακομιστών βάσεων δεδομένων (database servers) των Μονάδων Υγείας με τον διακομιστή επικοινωνίας (communication server) της 7ης ΥΠΕ.

Ο χρήστης, αφού πιστοποιηθεί, επιλέγει την σελίδα που θέλει να ανοίξει, κάνοντας μία αίτηση στον διακομιστή εφαρμογών του συστήματος, ο οποίος αφού αναλύσει την αίτηση, αντλεί στοιχεία είτε από τον διακομιστή βάσης δεδομένων, είτε στέλνει ένα αίτημα λήψης δεδομένων προς τον διακομιστή επικοινωνίας, είτε και τα δύο. Σε κάθε περίπτωση, ο διακομιστής εφαρμογών, αφού λάβει τα απαιτούμενα δεδομένα, τα μορφοποιεί σύμφωνα με τις απαιτήσεις της αίτησης του χρήστη και τα στέλνει στον χρήστη μέσω ασφαλούς πρωτοκόλλου (https).

Η φυσική τοποθεσία τήρησης των δεδομένων είναι είτε κατανεμημένη στα διάφορα πληροφοριακά συστήματα των Μονάδων Υγείας είτε κεντρική στην 7η ΥΠΕ, ανάλογα με το είδος των δεδομένων. Ενδεικτικά, τα δημογραφικά στοιχεία των ασθενών/βασικά στοιχεία περιστατικών τηρούνται και τοπικά σε κάθε Μονάδα Υγείας αλλά και κεντρικά στην 7η ΥΠΕ. Τα στοιχεία του φακέλου υγείας καθώς και τα στοιχεία των εργαστηρίων τηρούνται κατανεμημένα στα πληροφοριακά συστήματα των Μονάδων Υγείας. Τα ενημερωτικά σημειώματα καθώς και πρόσθετες πληροφορίες για τον ασθενή (π.χ βιοψίες) τηρούνται κεντρικά στην 7η ΥΠΕ.

Περαιτέρω, στο υποβληθέν προαναφερόμενο υπόμνημα της 7ης ΥΠΕ περιγράφονται αναλυτικά τα τηρούμενα μέτρα ασφάλειας, μεταξύ των οποίων

αναφέρονται: Η πλήρης καταγραφή ενεργειών πρόσβασης χρηστών , διαχειριστών και κρυπτογράφηση της βάσης δεδομένων. Τα συνθηματικά των χρηστών καθώς και τα βασικά στοιχεία ασθενών είναι πρόσθετα κρυπτογραφημένα. Έχει οριστεί ελάχιστο μήκος συνθηματικών και υποχρέωση τακτικής αλλαγής για χρήστες και διαχειριστές, καθώς και άμεση απενεργοποίηση μετά από συγκεκριμένο αριθμό αποτυχημένων προσπαθειών. Έχουν ληφθεί μέτρα για αποφυγή επιθέσεων με τεχνικές sql injections και επιθέσεων μορφής denial of service. Η νησίδα «Σύζευξις» της 7^{ης} ΥΠΕ είναι ένα προστατευμένο σύστημα δικτύωσης, ενώ δεν υπάρχει τρόπος σύνδεσης με την ΠΑΝΑΚΕΙΑ, απευθείας από το διαδίκτυο. Τηρούνται επίσης οι απαραίτητες προδιαγραφές ασφαλείας στο υπολογιστικό κέντρο όπου φιλοξενούνται οι διακομιστές του συστήματος.

Σχετικά με τη συγκατάθεση των ασθενών, προτείνεται από την 7^{η} ΥΠΕ η δημιουργία ενός μητρώου ασθενών οι οποίοι δεν επιθυμούν το ιατρικό προσωπικό να έχει πρόσβαση στο ιατρικό ιστορικό τους. Με την εισαγωγή μιας εγγραφής στο μητρώο, θα «κλειδώνει» το ιστορικό και ο ιατρός δεν θα μπορεί να δει καθόλου το ιστορικό του ασθενή, οπουδήποτε στην Κρήτη. Κατά τη διάρκεια της νοσηλείας ο γιατρός θα εισάγει κανονικά τα ιατρικά δεδομένα που παράγονται κατά τη νοσηλεία, στον ηλεκτρονικό ιατρικό του φάκελο. Ο ασθενής μπορεί αργότερα, σε άλλο περιστατικό της νοσηλείας του, να επιτρέψει την προβολή των ιατρικών του δεδομένων και έτσι ο γιατρός του, να μπορεί να δει το ιστορικό του, χωρίς καμία έλλειψη. Επιπρόσθετα, ο ασθενής μπορεί κατά το δοκούν να επιτρέπει ή να απαγορεύει την πρόσβαση στον ιατρικό του φάκελο, ανάλογα με την εμπιστοσύνη που έχει στον ιατρό που είναι απέναντί του. Πρόσθετο μέτρο αποτελεί ένα προειδοποιητικό μήνυμα (που θα εμφανίζεται άπαξ ανά περιστατικό), όπου θα ενημερώνεται ο ιατρός ότι πρέπει να έχει τη συγκατάθεση του ασθενούς, όταν αυτός επιχειρεί να προσπελάσει στοιχεία ιστορικού.

Σύμφωνα με το σύστημα ΠΑΝΑΚΕΙΑ, με την είσοδο του ασθενούς στη Μονάδα Υγείας για νοσηλεία, θα καλείται να υπογράψει φόρμα αποδοχής πρόσβασης (ή μη) στον ηλεκτρονικό ιατρικό του φάκελο. Θα καταχωρείται στο μητρώο η δήλωσή του και η εφαρμογή θα «διαβάζει» τη δήλωση αυτή και θα επιτρέπει ή μη την πρόσβαση στο ιατρονοσηλευτικό προσωπικό στον φάκελο υγείας του.

Η πολιτική πρόσβασης προβολής/συμπλήρωσης του ιατρικού φακέλου του ασθενή θα γίνεται με τη λογική «παραθύρου πρόσβασης», το οποίο μπορεί να βρίσκεται σε τρεις καταστάσεις:

- «πλήρως ανοικτό»: Με την εισαγωγή ενός ασθενή σε μία κλινική «ανοίγει πλήρως το παράθυρο πρόσβασης» και ο ιατρός της κλινικής έχει πρόσβαση να δει α. τα περιστατικά του ασθενή, β. τα ενημερωτικά σημειώματα που παρήχθησαν, γ. τις εργαστηριακές εξετάσεις, δ. αρχεία που έχουν καταχωρηθεί για τον ασθενή, ε. τον φάκελο υγείας του (αλλεργίες, χρόνια νοσήματα, κτλ). Όλα τα παραπάνω είναι από καταχωρήσεις που έχουν γίνει κατά το παρελθόν από οποιαδήποτε Μονάδα Υγείας της Κρήτης από κάθε κλινική. Δεν μπορεί όμως να δει τα στοιχεία νοσηλείας (πορεία νόσου, λογοδοσίες, κτλ) που έχουν παραχθεί από άλλες κλινικές για διαφορετικά περιστατικά νοσηλείας του ασθενή.
- «μερικώς ανοικτό» : Με την έξοδο του ασθενούς από την κλινική, το σύστημα μεταπίπτει στην κατάσταση του «μερικώς ανοικτού παραθύρου», η οποία διαρκεί από 30 ως 90 ημέρες, ανάλογα την κλινική. Σε αυτήν την κατάσταση, η κλινική χάνει το δικαίωμα προβολής εξετάσεων από παρελθόντα περιστατικά, δεν μπορεί πλέον να εισαγάγει φαρμακευτική αγωγή, να καταχωρήσει εγγραφές λογοδοσίας, ζωτικών, πορείας νόσου κτλ. Ουσιαστικά μπορεί να «δει» τις εργαστηριακές εξετάσεις μόνο του υπάρχοντος περιστατικού, τα παρελθόντα ενημερωτικά σημειώματα και τον φάκελο υγείας. Ο λόγος που υπάρχει αυτό το «παράθυρο» είναι για να διευκολύνει το ιατρικό προσωπικό στη σύνταξη του ενημερωτικού σημειώματος του περιστατικού, στη πιθανή συμπλήρωση του φακέλου υγείας και στην ολοκλήρωση κάποιων εξετάσεων που τα αποτελέσματά τους «φτάνουν» μετά την έξοδο του ασθενούς από την κλινική (π.χ. βιοψίες).
- «περίπου κλειστό» : Μετά από αυτήν την περίοδο, η κατάσταση γίνεται «περίπου κλειστό παράθυρο» όπου η κλινική μπορεί να δει μόνο ότι παρήχθη από αυτήν, χωρίς κανένα δικαίωμα παρέμβασης στο περιστατικό. Συνεπώς κλινικές δεν μπορούν καν να δουν το περιστατικό και τα στοιχεία του, αν δεν έχει «περάσει» από αυτές. Ενώ ακόμα και αν έχει περάσει από αυτές, στην τρίτη κατάσταση του «μερικώς κλειστού παραθύρου», μπορούν να δουν μόνο ότι παρήχθη από αυτές.

Η Αρχή, αφού άκουσε τους εισηγητές και τις διασαφηνίσεις των βοηθών εισηγητών οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν διεξοδικής συζήτησης, εκδίδει την ακόλουθη

Γ Ν Ω Μ Ο Δ Ο Τ Η Σ Η

1. Για την επεξεργασία ευαίσθητων δεδομένων από φορείς παροχής ιατρικής φροντίδας (πρωτοβάθμιας ή δευτεροβάθμιας) εφαρμόζεται καταρχήν η διάταξη της παρ. 2 στοιχ. δ΄ του άρθρου 7 ν. 2472/1997, σύμφωνα με την οποία η επεξεργασία επιτρέπεται, μετά από άδεια της Αρχής, και χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων - ασθενούς, όταν αυτή «*αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας*». Η παραπάνω διάταξη αφορά στην επεξεργασία δεδομένων υγείας που συλλέγονται κατά την παροχή υπηρεσιών υγείας σε σχέση με συγκεκριμένο περιστατικό νοσηλείας, χωρίς να εκτείνεται σε περιπτώσεις που, αν και ενδέχεται να διευκολύνουν ή/και να λειτουργούν επιβοηθητικά στην παροχή ιατρικής φροντίδας, δεν συνδέονται απολύτως με την παροχή της. Δηλαδή η ως άνω επεξεργασία δεδομένων υγείας επιτρέπεται χωρίς συγκατάθεση του ασθενούς μόνον σε σχέση με τη συλλογή, αποθήκευση και χρήση των δεδομένων που παράγονται κατά την αντιμετώπιση συγκεκριμένου περιστατικού υγείας.

Η λειτουργία συστήματος ηλεκτρονικού ιατρικού φακέλου συγκεντρώνει διάχυτη πληροφορία από τα επιμέρους πληροφοριακά συστήματα των Μονάδων Υγείας της 7^{ης} ΥΠΕ έτσι ώστε να είναι δυνατή από έναν ιατρό (πρόσωπο που παρέχει υπηρεσίες υγείας) η ανάκτηση πλήρους και επικαιροποιημένου ιατρικού ιστορικού των ασθενών. Αν και η πραγματοποιούμενη επεξεργασία αποτελεί μια σημαντική διευκόλυνση κατά την αναζήτηση πληροφορίας για τον ασθενή, δεν συγκαταλέγεται στο είδος της επιτρεπόμενης επεξεργασίας με βάση την προαναφερθείσα διάταξη της παρ. 2 στοιχ. δ

του άρθρου 7 ν. 2472/1997.

Η επεξεργασία θα επιτρεπόταν είτε με ειδική διάταξη νόμου, η οποία επιπλέον θα έπρεπε να είναι σύμφωνη με την Οδηγία 95/46/ΕΚ για την προστασία των προσωπικών δεδομένων, και εφόσον τέτοια διάταξη δεν υφίσταται[1], αφού η επεξεργασία αυτή είναι γενικώς επωφελής για το υποκείμενο και πραγματοποιείται με τις εγγυήσεις του ιατρικού απορρήτου, είναι επιτρεπτή μόνον εάν το υποκείμενο των δεδομένων έχει δηλώσει εγγράφως την ειδική συγκατάθεσή του, βάσει της παρ. 2 στοιχ. α' του άρθρου 7 ν. 2472/1997, και μάλιστα, έτσι ώστε να του παρέχεται το δικαίωμα της επιλογής[2].

Σε σχέση λοιπόν και με δεδομένα που παρήχθησαν από άλλες Μονάδες Υγείας, η πρόσβαση και χρήση των ιατρικών δεδομένων από τους θεράποντες ιατρούς του τρέχοντος περιστατικού προϋποθέτει τη συγκατάθεση του ασθενούς, τα ιδιαίτερα χαρακτηριστικά της οποίας αναλύονται ακολούθως στην επόμενη σκέψη.

2. Σύμφωνα με το άρθρο 2 στοιχ. ια' ν. 2472/1997 η συγκατάθεση για να είναι ισχυρή θα πρέπει να είναι ελεύθερη, ρητή και ειδική. Επιπλέον, ο ασθενής – υποκείμενο των δεδομένων - θα πρέπει να έχει προηγουμένως ενημερωθεί με τρόπο σαφή και να τελεί εν πλήρη επιγνώσει αυτής. Η ενημέρωση περιλαμβάνει τις πληροφορίες σχετικά με την ταυτότητα του υπευθύνου επεξεργασίας, το σκοπό της επεξεργασίας, τον τρόπο της επεξεργασίας (δηλαδή τη λειτουργία του συστήματος ΠΑΝΑΚΕΙΑ), τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, καθώς και την ύπαρξη του δικαιώματος πρόσβασης και τον τρόπο άσκησής του. Τέλος, η συγκατάθεση πρέπει να μπορεί να

[1] Η νομοθετική ρύθμιση του ν. 4238/2014 (ΦΕΚ Α΄38), άρθρο 51 παρ. 4, καθιερώνει τον ατομικό ηλεκτρονικό φάκελο υγείας (ΑΗΦΥ) για όλους τους πολίτες, όμως το σύστημα ΠΑΝΑΚΕΙΑ δεν αποτελεί την υλοποίηση της νομοθετικής αυτής πρόβλεψης, για την οποία εκκρεμεί η προβλεπόμενη από το εδ. 2 έκδοση της σχετικής υπουργικής απόφασης, για να καθιερωθεί το πρότυπο ΑΗΦΥ σχετικά με το περιεχόμενο, τον τρόπο κατάρτισης, την ταυτοποίηση του ατόμου και την πρόσβαση στις ιατρικές πληροφορίες του φακέλου (βλ. και άρθρα 9-11 του ν.3235/2004, ΦΕΚ Α΄ 53).

[2] Πβλ. και Έγγραφο Εργασίας WP 131 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία στο πλαίσιο των ηλεκτρονικών μητρώων υγείας (ΗΜΥ) της Ομάδας Εργασίας του Άρθρου 29 της Οδηγίας 95/46/ΕΚ (διαθέσιμο στη διεύθυνση http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_el.pdf). Το ίδιο σκεπτικό αναπτύσσεται και στο υπ' αριθμ. 01/2012 Έγγραφο Εργασίας της Ο.Ε. του Άρθρου 29 σχετικά με το ευρωπαϊκό πρόγραμμα epSOS, κεφάλαιο 3, σύμφωνα με το οποίο η βάση επεξεργασίας για τη διαβίβαση στοιχείων του ηλεκτρονικού φακέλου, ελλείψει ειδικής νομοθεσίας, είναι η συγκατάθεση του ασθενούς ή εφόσον υφίσταται ζωτικό συμφέρον του ασθενούς ή τρίτου προσώπου και ο ασθενής τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, (διαθέσιμο στη διεύθυνση http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp189_en.pdf).

ανακαλείται οποτεδήποτε, χωρίς βέβαια η ανάκληση να έχει αναδρομικό αποτέλεσμα.

Η συγκατάθεση μπορεί να δοθεί μία φορά, κατά την επίσκεψη σε Μονάδα Υγείας της 7ης ΥΠΕ. Προτείνεται ο ασθενής να μπορεί, εκτός από τη γενική συγκατάθεση που παρέχει για την επεξεργασία των δεδομένων του στο πλαίσιο της λειτουργίας του συστήματος ΠΑΝΑΚΕΙΑ, η υλοποίηση της οποίας περιγράφεται στο υποβληθέν υπόμνημα της 7ης ΥΠΕ, να έχει τη δυνατότητα να αποκλείει την πρόσβαση σε στοιχεία που έχουν εισαχθεί από συγκεκριμένες Μονάδες Υγείας ή και επιμέρους κλινικές. Επίσης, προτείνεται να δίδεται η δυνατότητα να εξαιρείται η πρόσβαση σε ιδιαιτέρως ευαίσθητα δεδομένα, όπως τα δεδομένα ψυχικής υγείας. Τέλος, πρέπει να σημειωθεί ότι σε περίπτωση επείγοντος περιστατικού, όπου κινδυνεύει η υγεία ή ζωή του ασθενούς και ο ίδιος τελεί σε νομική ή φυσική αδυναμία να δώσει τη συγκατάθεσή του η διάταξη του άρθρου 7 παρ. 2 στοιχ. β ν. 2472/1997 προβλέπει ότι επιτρέπεται η επεξεργασία, πάντα μόνον των αναγκαίων προς αντιμετώπιση του περιστατικού δεδομένων (βλ. και άρθρο 12 παρ. 3 ν.3418/2005). Συνεπώς, με βάση αυτή τη διάταξη θα ήταν επιτρεπτή η πρόσβαση σε δεδομένα άλλων κλινικών ή άλλων μονάδων υγείας, εφόσον ο ασθενής ενημερωθεί, κατά την πρώτη επίσκεψή του σε οποιαδήποτε μονάδα υγείας. Προς τούτο είναι χρήσιμο να προβλεφθούν, ώστε η ενημέρωση να είναι κατά το δυνατόν ειδική, τα υποσύνολα των δεδομένων που κρίνονται «ζωτικά» για την αντιμετώπιση επειγόντων και κρίσιμων για την υγεία ή τη ζωή του ασθενούς περιστατικών.

Η συγκατάθεση θα πρέπει να δίδεται με τη συμπλήρωση και υπογραφή ειδικού εντύπου, το οποίο θα είναι σαφές και εύληπτο για τον μέσο ασθενή. Επίσης, θα πρέπει ο ενδιαφερόμενος ασθενής – υποκείμενο των δεδομένων – να ενημερώνεται για τη δυνατότητα αλλαγής των επιλογών του που σημαίνει τροποποίηση ή ανάκληση της συγκατάθεσης για το μέλλον, και να υπάρχει προς τούτο ειδικό έντυπο.

Μια πιο φιλική και ασφαλής εναλλακτική για τη χορήγηση της συγκατάθεσης λύση είναι ο εφοδιασμός των ασθενών με έξυπνη κάρτα[3], με την οποία ο ενδιαφερόμενος ασθενής μέσω της εισαγωγής κωδικού πρόσβασης σηματοδοτεί τη συγκατάθεσή του. Σε αυτή την περίπτωση, η συγκατάθεση θα πρέπει να δίδεται κάθε φορά και στην έκταση

[3] Επισημαίνεται ότι το άρθρο 9 παρ. 3 του ν. 3235/2004 (ΦΕΚ Α΄53) προβλέπει την έκδοση ηλεκτρονικής κάρτας υγείας του πολίτη, χωρίς ωστόσο να έχει εκδοθεί μέχρι σήμερα η προβλεπόμενη από την

που κάθε φορά αποφασίζει ο ασθενής, δηλαδή δεν απαιτείται η εκ των προτέρων επιλογή ανάμεσα στις διάφορες περιπτώσεις, όπως αυτές αναλύθηκαν ανωτέρω.

Οι επιλογές του ενδιαφερόμενου ασθενούς πρέπει να αντανακλώνται στο πληροφοριακό σύστημα ΠΑΝΑΚΕΙΑ, δηλαδή να υλοποιούνται τεχνικώς. Με άλλα λόγια, ο χρήστης του συστήματος θα πρέπει να έχει πρόσβαση στα δεδομένα ανάλογα με το είδος της συγκατάθεσης που έχει δώσει ο ασθενής. Για κάθε πρόσβαση σε δεδομένα για τα οποία δεν έχει δοθεί συγκατάθεση, το σύστημα πρέπει να απαιτεί νέα ειδική συγκατάθεση.

3. Σε περίπτωση που ο ασθενής τελεί σε νομική ή φυσική αδυναμία καθώς και όταν δεν έχει τη ικανότητα δικαιοπραξίας η συγκατάθεση για την πρόσβαση στο πλήρη ιατρικό φάκελο του ασθενούς δίδεται από το νόμιμο εκπρόσωπό του, σύμφωνα με τις οικείες διατάξεις του ΑΚ (π.χ. τους γονείς ή το γονέα που ασκεί τη γονική μέριμνα, το δικαστικό συμπαραστάτη).

4. Σύμφωνα με τα οριζόμενα στις διατάξεις των άρθρων 12 ν. 2472/1997 και 14 παρ. 8 του ν.3418/2005 ο ασθενής έχει δικαίωμα πρόσβασης στον ιατρικό του φάκελο το οποίο δεν εξαρτάται από προϋποθέσεις και το οποίο ο υπεύθυνος επεξεργασίας, οφείλει να ικανοποιεί χωρίς καθυστέρηση και με εύληπτο και σαφή τρόπο. Στην περίπτωση που ο ασθενής δεν έχει την ικανότητα δικαιοπραξίας, το δικαίωμα πρόσβασης ασκείται από το νόμιμο εκπρόσωπό του (δικαστικό συμπαραστάτη, γονείς ή γονέα που έχει τη γονική μέριμνα).

Το δικαίωμα αυτό δύναται να ασκηθεί σε κάθε Μονάδα Υγείας της Κρήτης ή και στην 7η ΥΠΕ, και να έχει πρόσβαση ο ασθενής σε όλα τα τηρούμενα δεδομένα.

5. Σύμφωνα με το άρθρο 4 παρ. 1 στοιχ. δ΄ του ν. 2472/1997, τα προσωπικά δεδομένα πρέπει να διατηρούνται μόνον για το χρονικό διάστημα που είναι απαραίτητο για την πραγματοποίηση του σκοπού της επεξεργασίας. Επισημαίνεται ότι το άρθρο 14 παρ. 4 περ. β’ ν. 3418/2005 (Κώδικας Ιατρικής Δεοντολογίας) υποχρεώνει τους δημόσιους φορείς παροχής πρωτοβάθμιας και δευτεροβάθμιας φροντίδας να τηρούν για μία εικοσαετία από την τελευταία επίσκεψη του ασθενούς αρχείο με ορισμένα στοιχεία κατά την παρ. 2 και 3 της ίδιας διάταξης, που στην περίπτωση μονάδων δευτεροβάθμιας

παράγραφο 5 υπουργική απόφαση που καθορίζει ουσιώδη στοιχεία αυτής.

φροντίδας, δηλαδή κλινικών και νοσοκομείων, περιλαμβάνουν τα αποτελέσματα των κλινικών και παρακλινικών εξετάσεων. Οι ρυθμίσεις αυτές του ΚΙΔ για τον χρόνο τήρησης ισχύουν και για τα δεδομένα υγείας που τυγχάνουν επεξεργασίας μέσω του εξεταζόμενου συστήματος ΠΑΝΑΚΕΙΑ.

Μετά το πέρας της χρονικής διάρκειας τήρησης των δεδομένων πρέπει αυτά να καταστρέφονται με ασφαλή τρόπο, δηλαδή η υποχρέωση λήψης των κατάλληλων μέτρων ασφάλειας κατά το άρθρο 10 ν. 2472/1997 υφίσταται μέχρι και την καταστροφή των δεδομένων. Για το σκοπό αυτό η Αρχή έχει εκδώσει την Οδηγία 1/2005 (διαθέσιμη στην ιστοσελίδα της Αρχής), η οποία παρέχει κατευθυντήριες γραμμές για την ασφαλή καταστροφή προσωπικών, καθώς και των ευαίσθητων, όπως εν προκειμένω, δεδομένων που τηρούνται σε έντυπη ή ηλεκτρονική μορφή.

6. Σύμφωνα με το άρθρο 2 στοιχ. ζ΄ του ν. 2472/1997 υπεύθυνος επεξεργασίας είναι όποιος «*…καθορίζει το σκοπό και τον τρόπο της επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και τρόπος καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο*.».

Η Οδηγία 95/46/ΕΚ περιέχει αντίστοιχο ορισμό στο άρθρο 2 στοιχ. δ) με μόνη διευκρινιστική προσθήκη -την οποία δεν αποκλείει το γράμμα και το πνεύμα του ελληνικού νόμου - ότι ο υπεύθυνος επεξεργασίας καθορίζει από μόνος του ή από κοινού με άλλους το σκοπό και τον τρόπο της επεξεργασίας, προβλέποντας έτσι ότι η πολυπλοκότητα των εννόμων σχέσεων και των συναλλακτικών και τεχνολογικών αναγκών μπορεί να οδηγεί σε περισσότερους υπευθύνους επεξεργασίας για την ίδια ή διαφορετική, επιμέρους εργασία στο ευρύτερο πλαίσιο της επεξεργασίας των προσωπικών δεδομένων κατά την έννοια του άρθρου 2 στοιχ. δ΄ του ν. 2472/1997.

Στην υπό εξέταση περίπτωση υπεύθυνο επεξεργασίας αποτελούν τόσο οι Μονάδες Υγείας, όσο και η 7η ΥΠΕ, της οποίας οι ρόλοι και αρμοδιότητες διέπονται από την ειδική νομοθεσία που διέπει τις Υγειονομικές Περιφέρειες της χώρας[4].

[4] Οι ΥΠΕ ιδρύθηκαν με το ν. 2889/2001 (ως ΠΕΣΥ), που τροποποιήθηκε με το ν. 3106/2003 (ως ΠΕΣΥΠ), που τροποποιήθηκε με το ν. 3329/2005 (ως ΔΥΠΕ), που τροποποιήθηκε με το ν. 3527/2007 (ως ΥΠΕ).

Οι Μονάδες Υγείας αποτελούν υπεύθυνο επεξεργασίας για τα δεδομένα υγείας των ασθενών τα οποία τηρούνται στο ΟΠΣΥ Κρήτης για τον σκοπό της παροχής υπηρεσιών υγείας.

Η 7η ΥΠΕ αποτελεί υπεύθυνο επεξεργασίας του πληροφοριακού συστήματος ΠΑΝΑΚΕΙΑ, καθώς σε αυτή συγκεντρώνονται δεδομένα κατ' εντολήν της από τις Μονάδες Υγείας (π.χ ενημερωτικά σημειώματα, βιοψίες). Η 7η ΥΠΕ αποτελεί επίσης υπεύθυνο επεξεργασίας του πληροφοριακού συστήματος ΠΑΝΑΚΕΙΑ γιατί καθορίζει τον σκοπό της επεξεργασίας και τη λειτουργία του εν λόγω συστήματος και ελέγχει και εποπτεύει από τον νόμο τις Μονάδες Υγείας. Επιπλέον δε παρέχει τα μέσα (κεντρική πληροφοριακή υποδομή) μέσω των οποίων πραγματοποιείται η τήρηση των δεδομένων υγείας των ασθενών από κάθε μονάδα υγείας.

Συνεπώς, οι ως άνω υπεύθυνοι επεξεργασίας, 7^{η} ΥΠΕ και Μονάδες Υγείας, οφείλουν να εκπληρώσουν τις υποχρεώσεις που απορρέουν από τις διατάξεις των άρθρων 6, 7 παρ. 2 στοιχ. α΄ και 7^{Α} παρ. 1 στοιχ. δ΄ τελ. εδάφιο του ν. 2472/1997.

7. Σύμφωνα με το άρθρο 10 παρ. 3 του ν. 2472/1997: «*Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας…*». Η υποχρέωση αυτή βαρύνει αναλόγως και τον εκτελούντα την επεξεργασία, σύμφωνα με την παρ. 4 του ιδίου άρθρου του παραπάνω νόμου.

Όσον αφορά τα τεχνικά θέματα της αρχιτεκτονικής του συστήματος ΠΑΝΑΚΕΙΑ, καθώς και τα τηρούμενα μέτρα ασφάλειας (άρθρο 10 του ν.2471/1997), πρέπει να λεχθούν τα εξής:

α) Συνίσταται να εκπονηθεί σύστημα διαχείρισης ασφάλειας πληροφοριών (ΣΔΑΠ)

Επισημαίνεται, περαιτέρω, ότι σύμφωνα με τα οριζόμενα στη διάταξη του άρθρου 2 παρ. 2 του ν. 4238/2014 τα Κέντρα Υγείας της χώρας με τις αποκεντρωμένες μονάδες τους (πολυδύναμα περιφερειακά ιατρεία, περιφερειακά ιατρεία, ειδικά περιφερειακά ιατρεία) μεταφέρθηκαν και εντάχθηκαν στην οργανωτική δομή των οικείων ΔΥΠε και αποτελούν αποκεντρωμένες οργανικές μονάδες τους.

για το πληροφοριακό σύστημα ΠΑΝΑΚΕΙΑ, το οποίο συνιστάται να ακολουθεί διεθνή πρότυπα (π.χ τη σειρά προτύπων διαχείρισης ασφάλειας πληροφοριών ISO 27000, με το γενικό πρότυπο να είναι το ISO 27001:2013 και το ειδικότερο πρότυπο να είναι το ISO 27799:2008 που αφορά τα συστήματα υγείας). Το ΣΔΑΠ περιλαμβάνει τα ακόλουθα τέσσερα στάδια (κύκλος ζωής): 1. Καθιέρωση και σχεδίαση του ΣΔΑΠ, στη βάση σχετικής μελέτης επικινδυνότητας και κατάλληλης πολιτικής ασφάλειας, 2. Υλοποίηση και λειτουργία του ΣΔΑΠ, καθώς και εκπαίδευση του ανθρώπινου δυναμικού, 3. Συνεχής παρακολούθηση και περιοδικός έλεγχος της ορθής λειτουργίας και αξιολόγηση της αποτελεσματικότητας του ΣΔΑΠ, 4. Συντήρηση και βελτίωση του ΣΔΑΠ.

Οι προβλεπόμενες ενέργειες και τα αποτελέσματά τους, καθώς και οι ακολουθούμενες διαδικασίες τεκμηριώνονται σε έντυπη ή/και ηλεκτρονική μορφή. Το ΣΔΑΠ περιλαμβάνει τουλάχιστον μελέτη επικινδυνότητας, πολιτική ασφάλειας και ειδικά (τεχνικά και οργανωτικά) μέτρα ασφάλειας σχετικά με την εσωτερική οργάνωση και τη διαχείριση των αγαθών, το εμπλεκόμενο ανθρώπινο δυναμικό, το φυσικό περιβάλλον λειτουργίας, τον κύκλο ζωής των δεδομένων, συστημάτων και υπηρεσιών (διαχείριση δεδομένων και διαχείριση λειτουργίας συστημάτων και υπηρεσιών, προμήθεια ή/και ανάπτυξη, εγκατάσταση και συντήρηση), τον έλεγχο πρόσβασης, τη διαχείριση συνέχισης λειτουργίας (business continuity management) και τη διαχείριση περιστατικών ασφάλειας. Η αποτελεσματική λειτουργία των καθορισμένων οργανωτικών και τεχνικών μέτρων πρέπει να ελέγχεται περιοδικά.

β) Θα πρέπει να υποβληθεί στην Αρχή κείμενο κώδικα δεοντολογίας σχετικά με την προστασία των προσωπικών δεδομένων που τηρεί ο υπεύθυνος επεξεργασίας (7η ΥΠΕ).

γ) Θα πρέπει να οριστεί εσωτερικός υπεύθυνος προστασίας προσωπικών δεδομένων (αναφέρεται και στο άρθρο 36 παρ. 2 του ν. 3979/2011 για την ηλεκτρονική διακυβέρνηση), ο οποίος θα μεριμνά για τη λήψη όλων των αναγκαίων τεχνικών και οργανωτικών μέτρων για την τήρηση των αρχών και υποχρεώσεων ως προς την επεξεργασία προσωπικών δεδομένων, όπως η υιοθέτηση και εφαρμογή πολιτικής ασφαλείας, η περιοδική κατάρτιση και ευαισθητοποίηση των υπαλλήλων ως προς την προστασία δεδομένων προσωπικού χαρακτήρα, η πρόταση για λήψη εσωτερικών διαδικασιών ελέγχου και επαλήθευσης της αποτελεσματικής εφαρμογής των μέτρων

ασφάλειας.

Θα πρέπει να ληφθεί υπόψη επίσης από την 7η ΥΠΕ καθώς και από τις Μονάδες Υγείας η ανάγκη εφαρμογής επιμέρους διατάξεων του ν. 3979/2011 για την ηλεκτρονική διακυβέρνηση καθώς και της υπουργικής απόφασης υπ' αρ. ΥΑΠ/φ.40.1/989/12.04.2012 (ΦΕΚ Β' 1301) για την κύρωση του πλαισίου παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης, ιδίως το άρθρο 1 παρ. 25 και το παράρτημα ΙΙ της υπουργικής απόφασης σχετικά με τους κανόνες και τα πρότυπα για τη διαλειτουργικότητα σε οργανωτικό, σημασιολογικό και τεχνολογικό επίπεδο για την ανταλλαγή των δεδομένων μεταξύ πληροφορικών συστημάτων των φορέων του δημοσίου τομέα. Το ίδιο ισχύει και σε σχέση με το ζήτημα της διαβαθμισμένης πρόσβασης των χρηστών και την αυθεντικοποίηση.

Οι απαιτήσεις ασφαλείας που καταγράφονται στο παράρτημα της παρούσας Γνωμοδότησης είναι ενδεικτικές, και θα πρέπει να καλύπτονται στο ΣΔΑΠ για το πληροφοριακό σύστημα ΠΑΝΑΚΕΙΑ, στο βαθμό που αυτές εφαρμόζονται στο εν λόγω σύστημα και πάντα ως απόρροια μελέτης επικινδυνότητας της υπολογιστικής και επικοινωνιακής υποδομής του συστήματος. Οι απαιτήσεις αυτές πρέπει επίσης να ικανοποιούνται και από τις Μονάδες Υγείας της 7ης ΥΠΕ, η ασφάλεια των πληροφοριακών συστημάτων των οποίων είναι απαραίτητη προκειμένου να εξασφαλίζεται η σωστή λειτουργία του συστήματος ΠΑΝΑΚΕΙΑ. [5]

Ο Πρόεδρος **Η Γραμματέας**

Π. Χριστόφορος **Ε. Παπαγεωργοπούλου**

[5] Σημειώνεται ότι τις απαιτήσεις αυτές έχει επιβάλει η Αρχή σε νοσηλευτικά ιδρύματα με τις υπ' αριθμ. 35 έως 44 αποφάσεις της του έτους 2011 με τις οποίες εγκρίθηκαν τα πορίσματα 10 διοικητικών ελέγχων.

ΠΑΡΑΡΤΗΜΑ

1. Υπεύθυνος ασφαλείας

Ο υπεύθυνος ασφαλείας έχει σημαντικό ρόλο σε έναν οργανισμό, καθώς είναι εκείνος που ελέγχει την εφαρμογή των οργανωτικών και τεχνικών μέτρων ασφαλείας, όπως αυτά έχουν επιλεγεί σύμφωνα με το άρθρο 10 του ν. 2472/12977 και έχουν αποτυπωθεί στην πολιτική και στο σχέδιο ασφαλείας.

Ο υπεύθυνος επεξεργασίας οφείλει να ορίσει εγγράφως υπεύθυνο ασφαλείας των προσωπικών δεδομένων με συγκεκριμένες αρμοδιότητες.

Ο υπεύθυνος ασφαλείας πρέπει τουλάχιστον να έχει την επίβλεψη της κατάρτισης και της εφαρμογής της πολιτικής και του σχεδίου ασφαλείας, να προτείνει σχετικές αναθεωρήσεις όταν αυτό χρειάζεται.

Ο υπεύθυνος ασφαλείας πρέπει να διαθέτει τα απαραίτητα επαγγελματικά προσόντα από πλευράς τεχνικών γνώσεων (π.χ. γνώσεων συστημάτων πληροφορικής) και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

2. Σχέδιο ανάκαμψης από καταστροφές

Το σχέδιο ανάκαμψης από καταστροφές είναι απαραίτητο για την αποτύπωση των διαδικασιών και των τεχνικών μέτρων που πρέπει να εφαρμόσει ο υπεύθυνος επεξεργασίας για την προστασία των προσωπικών δεδομένων σε περίπτωση κάποιου έκτακτου περιστατικού, όπως φυσικές καταστροφές (π.χ. σεισμός, πυρκαγιά, πλημμύρα) ή μεγάλης εμβέλειας περιστατικά ασφαλείας (π.χ. καταστροφή από ιομορφικό λογισμικό). Ως εκ τούτου, συμπληρώνει το σχέδιο ασφαλείας (ή αποτελεί μέρος του).

Ο υπεύθυνος επεξεργασίας οφείλει να εκπονήσει σχέδιο ανάκαμψης από καταστροφές. Το σχέδιο πρέπει να περιγράφει τις βασικές διαδικασίες που ακολουθούνται για την προστασία των προσωπικών δεδομένων σε περιπτώσεις εκτάκτων περιστατικών. Ειδικότερα, πρέπει τουλάχιστον να περιγράφει τις συνθήκες και τα περιστατικά ασφαλείας κάτω από τα οποία ενεργοποιείται (το σχέδιο), να ορίζει τους

σχετικούς ρόλους και αρμοδιότητες του προσωπικού, καθώς και τρόπους αντιμετώπισης των περιστατικών που καλύπτει.

Το σχέδιο πρέπει να επικαιροποιείται μετά από κάθε σημαντική αλλαγή στο πληροφοριακό σύστημα αλλά και σε τακτική βάση.

Πρέπει επίσης να ορίζονται και να εκτελούνται οι δοκιμές σεναρίων που περιγράφονται στο σχέδιο.

Τέλος, το σχέδιο πρέπει να φέρει την επίσημη ενυπόγραφη έγκριση της Διοίκησης του υπεύθυνου επεξεργασίας

3. Υποχρέωση εμπιστευτικότητας του προσωπικού

Σύμφωνα με την παρ. 2 του άρθρου 10 του ν. 2472/1997, ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Για το σκοπό αυτό, είναι απαραίτητη η λήψη ειδικών μέτρων από τον υπεύθυνο επεξεργασίας για την δέσμευση του προσωπικού που επεξεργάζεται προσωπικά δεδομένα ως προς την εμπιστευτικότητα, ιδίως όταν το εν λόγω προσωπικό δεν δεσμεύεται ήδη από απόρρητο (όπως π.χ. το ιατρικό και νοσηλευτικό). Ένα τέτοιο μέτρο είναι η σύνταξη κωδίκων δεοντολογίας, οι οποίοι πρέπει να καθορίζουν τις βασικές αρχές προστασίας προσωπικών δεδομένων και να είναι δεσμευτικές -μέσω πράξης της διοικήσεως- για το προσωπικό (είτε ως εξειδίκευση των καθηκόντων του προσωπικού, είτε ως μέρος της σύμβασής του).

α) Οι υπάλληλοι (μόνιμοι, συμβασιούχοι, εποχικοί), καθώς και οι εξωτερικοί συνεργάτες που εξουσιοδοτούνται να έχουν πρόσβαση σε προσωπικά δεδομένα πρέπει να δεσμεύονται εγγράφως σχετικά με την τήρηση της εχεμύθειας και της εμπιστευτικότητας κατά τη διάρκεια της απασχόλησης και μετά την αποχώρησή τους, πριν την ενεργοποίηση της σχετικής πρόσβασης.

β) Ο υπεύθυνος επεξεργασίας οφείλει να καταρτίζει κώδικα δεοντολογίας με τις βασικές αρχές προστασίας προσωπικών δεδομένων που πρέπει να ακολουθούν οι υπάλληλοι (μόνιμοι, συμβασιούχοι, εποχικοί), καθώς και οι εξωτερικοί συνεργάτες Ο

κώδικας πρέπει να φέρει την έγκριση της διοίκησης του υπεύθυνου επεξεργασίας και να είναι δεσμευτικός για τους υπαλλήλους (π.χ. ως πράξη της διοίκησης που εξειδικεύει τα καθήκοντα των υπαλλήλων ή ως τμήμα της σύμβασης των υπαλλήλων με τον υπεύθυνο επεξεργασίας). Ο κώδικας δεοντολογίας πρέπει, μεταξύ άλλων, να καθορίζει πιθανές κυρώσεις σε περίπτωση παραβίασής του, να ορίζει την ύπαρξη Επιτροπής Δεοντολογίας, τις αρμοδιότητές της και τον τρόπο επικοινωνίας με αυτή και, τέλος, να περιλαμβάνει διαδικασία αναθεώρησής του.

4. Διαχείριση πληροφοριακών αγαθών

Η ορθή διαχείριση του υλικού και του λογισμικού, καθώς και των πόρων του δικτύου παίζει κεντρικό ρόλο στην ασφαλή διαχείριση των προσωπικών δεδομένων, καθώς επιτρέπει τον έλεγχο των μέσων βάσει των οποίων πραγματοποιείται η επεξεργασία, καθώς και των μέτρων ασφαλείας που εφαρμόζονται σε αυτά (τα μέσα). Η διαχείριση πληροφοριακών αγαθών περιλαμβάνει τουλάχιστον την καταγραφή του εξοπλισμού (ηλεκτρονικού ή μη, σταθερού ή φορητού) και της τοπολογίας του δικτύου μέσω των οποίων πραγματοποιείται επεξεργασία προσωπικών δεδομένων.

α) Ο υπεύθυνος επεξεργασίας πρέπει να καταγράφει τα πληροφοριακά αγαθά σε επαρκές επίπεδο ανάλυσης (κατάλογος πληροφοριακών αγαθών).

Ο κατάλογος των πληροφοριακών αγαθών πρέπει να περιλαμβάνει και τα εκτός παραγωγής συστήματα (π.χ. εξυπηρετητές παλαιότερου πληροφοριακού συστήματος).

Η καταγραφή του εξοπλισμού πρέπει να αναθεωρείται τακτικά, π.χ. σε ετήσια βάση. Ενδεικτικά, η καταγραφή μπορεί να περιλαμβάνει: το πληροφοριακό αγαθό, τη μορφή του αγαθού (π.χ. server, τερματικό χρήστη), την τοποθεσία του (φυσική ή/και ηλεκτρονική), τους ρόλους που έχουν δικαίωμα πρόσβασης στο αγαθό, καθώς και το είδος των προσωπικών δεδομένων που υφίστανται επεξεργασία.

Η καταγραφή του εξοπλισμού πρέπει να ελέγχεται από συγκεκριμένο εξουσιοδοτημένο πρόσωπο (π.χ. τον διαχειριστή του πληροφοριακού συστήματος ή/και τον υπεύθυνο ασφαλείας).

5. Διαχείριση χρηστών

Η ορθή διαχείριση των χρηστών αποτελεί τόσο οργανωτικά, όσο και τεχνικά, ένα βασικό μέτρο ασφάλειας, σύμφωνα με το άρθρο 10 του ν. 2472/1997, για την απόδοση δικαιωμάτων πρόσβασης των υπαλλήλων του υπεύθυνου επεξεργασίας στο πληροφοριακό του σύστημα. Ειδικότερα, οι υπάλληλοι πρέπει να έχουν πρόσβαση αποκλειστικά στα δεδομένα που απαιτούνται για την πραγματοποίηση της εργασίας τους, καθώς και στους σχετικούς με αυτά πόρους του συστήματος. Για τον σκοπό αυτό είναι απαραίτητη η υιοθέτηση μίας συγκεκριμένης πολιτικής αναφορικά με τη διαχείριση των χρηστών, η οποία πρέπει να υλοποιείται τεχνικά στο πλαίσιο του πληροφοριακού συστήματος.

Ο υπεύθυνος επεξεργασίας οφείλει να υιοθετήσει συγκεκριμένη πολιτική διαχείρισης των χρηστών του πληροφοριακού συστήματος, η οποία πρέπει να περιλαμβάνει τουλάχιστον

α) διαδικασία για εισαγωγή νέου χρήστη ή για μεταβολή των δικαιωμάτων των χρηστών (π.χ. κατά τη μετάθεση υπαλλήλου) στο σύστημα,

β) διαδικασία για τη διαγραφή μη ενεργού χρήστη (π.χ. σε περίπτωση αποχώρησης υπαλλήλου),

γ) κατηγοριοποίηση των χρηστών σε ομάδες ανάλογα με τα δικαιώματα πρόσβασης που αυτοί έχουν στους πόρους του συστήματος.

Ειδικά ως προς το τελευταίο, θα πρέπει να οριστούν οι κατάλληλοι ρόλοι και αντίστοιχα δικαιώματα χρηστών ανάλογα με τις αρμοδιότητες που έχουν αυτοί στο πλαίσιο λειτουργίας του συστήματος επεξεργασίας των δεδομένων (π.χ. διαφορετικοί ρόλοι για το ιατρικό προσωπικό και το προσωπικό της γραμματείας).

Η πολιτική πρέπει να μην επιτρέπει στους χρήστες να έχουν δικαιώματα διαχειριστή («administrator») στα τερματικά τους (το δικαίωμα αυτό πρέπει να εκχωρείται μόνο στους διαχειριστές του πληροφοριακού συστήματος).

Η πολιτική πρέπει να καλύπτει τόσο τους υπαλλήλους του υπεύθυνου επεξεργασίας, όσο και εξωτερικούς υπαλλήλους (π.χ. υπαλλήλους εκτελούντων την επεξεργασία που έχουν πρόσβαση στο πληροφοριακό σύστημα).

Ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι οι χρήστες έχουν πρόσβαση αποκλειστικά στις εφαρμογές και στα δεδομένα τα οποία απαιτούνται για την εκτέλεση της εργασίας τους και όχι σε παραπάνω.

6. Εκτελούντες την επεξεργασία

Σύμφωνα με το άρθρο 10 παρ. 1 και 4 του ν. 2472/1997, η επεξεργασία των προσωπικών δεδομένων είναι δυνατό να ανατεθεί σε εκτελούντα την επεξεργασία κατά την έννοια του στοιχ. η) του αρ. 2 του ίδιου νόμου. Στην περίπτωση αυτή, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως και προβλέπει ότι ο εκτελών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του άρθρου 10 ως προς την ασφάλεια βαρύνουν αναλόγως και αυτόν (τον εκτελούντα).

α) Ο υπεύθυνος επεξεργασίας οφείλει να συνάπτει τις συμβάσεις που αφορούν επεξεργασία προσωπικών δεδομένων εγγράφως με τους εκτελούντες την επεξεργασία. Οι συμβάσεις πρέπει να περιέχουν κατ' ελάχιστο τα παρακάτω: περιγραφή των προσωπικών δεδομένων, τον σκοπό, τον τόπο και τον τρόπο/διαδικασία της επεξεργασίας, καθώς και τα επίπεδα των υπηρεσιών που πρέπει να επιτυγχάνει ο εκτελών την επεξεργασία (σε επίπεδο ασφάλειας και ποιότητας δεδομένων). Οι συμβάσεις πρέπει να περιέχουν επίσης διαδικασίες ελέγχου συμμόρφωσης των διαδικασιών του εκτελούντα με τα προβλεπόμενα στη σύμβαση, καθώς και τις ρήτρες αναφορικά με παραβιάσεις όρων της σύμβασης σε σχέση με όλα τα ανωτέρω. Ο υπεύθυνος επεξεργασίας οφείλει να διασφαλίσει ότι ο εκτελών την επεξεργασία τηρεί τους όρους της πολιτικής ασφάλειας του (του υπεύθυνου) στο μέτρο που αυτή τον αφορά (τον εκτελούντα), όπως π.χ. αναφορικά με κανόνες πρόσβασης στα συστήματα, διαχείριση περιστατικών ασφαλείας, μέτρα φυσικής ασφάλειας, κλπ. Όταν η επεξεργασία γίνεται εκτός των εγκαταστάσεων του υπεύθυνου επεξεργασίας, ο υπεύθυνος θα πρέπει να εξασφαλίζει ότι ο εκτελών παρέχει επίπεδο ασφαλείας τουλάχιστον ανάλογο με αυτό που ορίζεται στην πολιτική ασφάλειας του υπευθύνου.

β) Οι υπάλληλοι του εκτελούντος που επεξεργάζονται, κατά το χρονικό διάστημα της σύμβασης, προσωπικά δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας πρέπει να δεσμεύονται εγγράφως με κατάλληλη δήλωση εμπιστευτικότητας.

7. Καταστροφή δεδομένων

Σύμφωνα με το άρθρο 4 παρ. 1 στοιχ. δ) του ν. 2472/1997, τα προσωπικά δεδομένα πρέπει να καταστρέφονται μετά το τέλος της περιόδου του απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Σύμφωνα με το αρ. 10 παρ. 2 του ν. 2472/1997, η καταστροφή πρέπει να γίνεται με ασφαλή τρόπο. Η Αρχή έχει εκδώσει την Οδηγία 1/2005, η οποία παρέχει κατευθυντήριες γραμμές για την ασφαλή καταστροφή προσωπικών δεδομένων σε έντυπη και ηλεκτρονική μορφή.

α) Πριν την καταστροφή εντύπων ή ηλεκτρονικών αρχείων που περιέχουν προσωπικά δεδομένα, καθώς και πριν την καταστροφή ή επαναχρησιμοποίηση εξοπλισμού στον οποίο είναι αποθηκευμένα αρχεία με προσωπικά δεδομένα, θα πρέπει να λαμβάνονται τα κατάλληλα μέτρα ώστε να διασφαλίζεται η πλήρης και μόνιμη διαγραφή των δεδομένων. Ειδικότερα, θα πρέπει να ακολουθούνται κατ' ελάχιστον όσα προβλέπονται στην Οδηγία 1/2005 της Αρχής για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας

β) Ο υπεύθυνος επεξεργασίας οφείλει να διαθέτει συγκεκριμένη γραπτή διαδικασία για την καταστροφή των δεδομένων, τόσο όταν πρόκειται για προγραμματισμένη μαζική καταστροφή δεδομένων, όσο και όταν πρόκειται για καταστροφή δεδομένων σε καθημερινή βάση (π.χ. με χρήση καταστροφέων εγγράφων), και να ενημερώνει σχετικά τους υπαλλήλους του.

8. Διαχείριση αλλαγών

Η διαχείριση αλλαγών στοχεύει στον συντονισμό και έλεγχο όλων των αλλαγών που πραγματοποιούνται στο πληροφοριακό σύστημα. Στο πλαίσιο της ασφάλειας το μέτρο αυτό είναι ιδιαίτερα σημαντικό, καθώς μια ανεπιτυχής εισαγωγή αλλαγής σε πληροφοριακό σύστημα το οποίο χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων, μπορεί να οδηγήσει σε αλλοίωση, καταστροφή ή αποκάλυψη δεδομένων σε μη εξουσιοδοτημένα πρόσωπα.

Ο υπεύθυνος επεξεργασίας πρέπει να ορίσει διαδικασία διαχείρισης αλλαγών των

συστημάτων επεξεργασίας προσωπικών δεδομένων. Κατ' ελάχιστο η εν λόγω διαδικασία πρέπει να περιέχει: καταγραφή των αιτημάτων αλλαγής, καθορισμό των ρόλων που έχουν δικαίωμα έγκρισης των αλλαγών, καθορισμό των κριτηρίων αποδοχής της αλλαγής και χρονοδιάγραμμα υλοποίησης. Στις περιπτώσεις που πραγματοποιείται ανάπτυξη λογισμικού, πρέπει αυτό να γίνεται σε περιβάλλον δοκιμών, το οποίο πρέπει να είναι απομονωμένο από το παραγωγικό σύστημα και επικαιροποιημένο. Τόσο κατά την ανάπτυξη του λογισμικού όσο και κατά την δοκιμή του τα χρησιμοποιούμενα δεδομένα θα πρέπει να είναι μη πραγματικά (dummy data). Αν είναι αναγκαίο να χρησιμοποιηθούν πραγματικά δεδομένα, μπορούν να χρησιμοποιηθούν μόνο σε ανωνυμοποιημένη μορφή.

9. Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων

Ως περιστατικό παραβίασης προσωπικών δεδομένων θεωρείται κάθε περίπτωση παραβίασης της ασφάλειας των δεδομένων στο πλαίσιο του χρησιμοποιούμενου συστήματος επεξεργασίας, όπως τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Στην περίπτωση ενός τέτοιου συμβάντος είναι απαραίτητο ο υπεύθυνος επεξεργασίας να διαθέτει τις κατάλληλες διαδικασίες, τόσο για την αναγνώρισή του, όσο και για την άμεση αντιμετώπισή του.

Ο υπεύθυνος επεξεργασίας πρέπει να ορίσει διαδικασία διαχείρισης περιστατικών παραβίασης προσωπικών δεδομένων. Κατ' ελάχιστο η διαδικασία πρέπει να ορίζει τις περιπτώσεις που θεωρούνται περιστατικά παραβίασης προσωπικών δεδομένων και να περιγράφει τον τρόπο αναφοράς των περιστατικών (από υπαλλήλους του υπεύθυνου επεξεργασίας ή/και εκτελούντες την επεξεργασία), τον τρόπο λήψης μέτρων για την αντιμετώπισή τους, καθώς και ενδεχόμενη διαδικασία ενημέρωσης των θιγόμενων ατόμων ανάλογα με την έκταση του περιστατικού. Τέλος, μέρος της διαδικασίας αποτελεί και η καταχώρηση των περιστατικών σε ειδικό αρχείο (έντυπο ή ηλεκτρονικό), το οποίο θα πρέπει να περιέχει τα βασικά χαρακτηριστικά του περιστατικού, καθώς και τον τρόπο με τον οποίο αντιμετωπίστηκε.

10. Εκπαίδευση του προσωπικού

Η εκπαίδευση του προσωπικού σε θέματα προστασίας προσωπικών δεδομένων, καθώς και σε ειδικές σχετικές με ασφάλεια λειτουργίες του πληροφοριακού συστήματος (π.χ. χρήση κωδικών πρόσβασης και συνθηματικών) είναι ιδιαιτέρως σημαντική για την ορθή εφαρμογή των οργανωτικών και τεχνικών μέτρων ασφαλείας.

α) Ο υπεύθυνος επεξεργασίας οφείλει να παρέχει συνεχή εκπαίδευση και ενημέρωση των υπαλλήλων σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας. Ειδικότερα, κατά την πρόσληψη πρέπει να κοινοποιεί στους υπαλλήλους την πολιτική ασφάλειας και τον κώδικα δεοντολογίας, καθώς και να τους ενημερώνει για τις ειδικές απαιτήσεις ασφάλειας ανάλογα με τον ρόλο και τις αρμοδιότητές τους μέσα στον οργανισμό. Επίσης, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει τους υπαλλήλους για σημαντικές αλλαγές των διαδικασιών ασφάλειας ή/και την εμφάνιση σημαντικών ζητημάτων ασφάλειας και προστασίας προσωπικών δεδομένων. Τέλος, θα πρέπει να παρέχεται διαρκής εκπαίδευση γύρω από τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας πληροφοριών στους διαχειριστές των συστημάτων και στους υπαλλήλους του Τμ. Πληροφορικής.

Ο υπεύθυνος επεξεργασίας είναι χρήσιμο να διαθέτει ορισμένο χρονοδιάγραμμα συνεχιζόμενης εκπαίδευσης των υπαλλήλων (ετήσιος χρονοπρογραμματισμός) σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας. Επίσης, συστήνεται η κατάρτιση ειδικότερων ενημερωτικών εντύπων για την ορθή χρήση του πληροφοριακού συστήματος και του διαδικτύου.

11. ***Προστασία χώρων εγκατάστασης πληροφορικού εξοπλισμού***

Τα φυσικά μέτρα ασφαλείας στοχεύουν στην προστασία των χώρων και των εγκαταστάσεων όπου γίνεται επεξεργασία προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση, καθώς και από ανθρώπινες ή φυσικές καταστροφές.

Οι χώροι εγκατάστασης πληροφορικού εξοπλισμού πρέπει να βρίσκονται σε απομονωμένο χώρο με ελεγχόμενη πρόσβαση, να διαθέτουν πόρτα ασφαλείας, κλιματισμό, πυρανίχνευση-πυρασφάλεια, ανιχνευτές υγρασίας και πλημμύρας καθώς και συστήματα αδιάλειπτης παροχής ενέργειας.

12. Σχεδιασμός πληροφοριακού συστήματος

Ο σχεδιασμός του πληροφοριακού συστήματος μέσω του οποίου πραγματοποιείται επεξεργασία προσωπικών δεδομένων πρέπει λαμβάνει υπόψη τις βασικές αρχές της ιδιωτικότητας κατά το σχεδιασμό (privacy by design) καθώς και της ιδιωτικότητας στις προεπιλεγμένες ρυθμίσεις (pricavy by default)..

Ως εκ τούτου, το σύστημα πρέπει, σύμφωνα με το αρ. 4 του ν. 2472/1997, να ακολουθεί την αρχή της ελαχιστοποίησης των δεδομένων (data minimization), δηλαδή να μην επιτρέπει την τήρηση προσωπικών δεδομένων ασθενών καθώς και χαρακτηρισμών εάν αυτό δεν είναι απολύτως απαραίτητο για την πραγματοποίηση του σκοπού επεξεργασίας. Θα πρέπει να δίνεται η δυνατότητα κωδικοποιημένης τήρησης χαρακτηρισμών ή ιδιαιτέρως ευαίσθητων δεδομένων. και οι προεπιλεγμένες ρυθμίσεις να είναι στην κατεύθυνση της ενίσχυσης της προστασίας προσωπικών δεδομένων δεδομένων.

Πρέπει επίσης να περιλαμβάνεται η δυνατότητα διαγραφής δεδομένων μετά το χρονικό διάστημα που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας.

Επίσης, σύμφωνα με το αρ. 10 του ν. 2472/1997, πρέπει να επιτρέπει την υλοποίηση όλων των απαιτούμενων τεχνικών μηχανισμών ασφαλείας για την προστασία των δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

.

13. Αναγνώριση και αυθεντικοποίηση

Οι μηχανισμοί αναγνώρισης και αυθεντικοποίησης, σε συνδυασμό με τις κατάλληλες

διαδικασίες διαχείρισης των χρηστών, αποτελούν βασικό μέτρο προστασίας από μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα. Όταν οι μηχανισμοί αυτοί βασίζονται στη χρήση κωδικών χρηστών και συνθηματικών (username – password), είναι απαραίτητο να υπάρχουν οι κατάλληλες διαδικασίες για τη διαχείριση των συνθηματικών, καθώς και άλλα σχετικά με αυτά μέτρα.

α) Πολιτική συνθηματικών: Ο υπεύθυνος επεξεργασίας οφείλει να υιοθετήσει συγκεκριμένη πολιτική διαχείρισης των συνθηματικών των χρηστών, η οποία πρέπει να περιλαμβάνει τουλάχιστον καθοδήγηση των χρηστών για το ελάχιστο μήκος και επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την ιστορικότητα του συνθηματικού, συχνότητα αλλαγής του συνθηματικού, μέγιστο αριθμό διαδοχικών επιτρεπτών/αποτυχημένων προσπαθειών πρόσβασης. Η πολιτική διαχείρισης των συνθηματικών πρέπει να ενσωματωθεί τεχνικά στις λειτουργίες του συστήματος.

β) Κοινόχρηστοι κωδικοί χρηστών: Ο υπεύθυνος επεξεργασίας πρέπει να αποφεύγει την απόδοση κοινόχρηστων κωδικών πρόσβασης σε ομάδες χρηστών. Στην περίπτωση που αυτό είναι απαραίτητο (π.χ. σε επείγοντα περιστατικά) πρέπει κατ’ ελάχιστον να διασφαλίζεται ότι οι εν λόγω χρήστες έχουν όλοι τους ίδιους ρόλους και αρμοδιότητες και κατ’ επέκταση τα ίδια δικαιώματα πρόσβασης στο σύστημα.

δ) Αυθεντικοποίηση βάσει ρόλου (κυρίως για τις εφαρμογές): Ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι οι χρήστες έχουν πρόσβαση αποκλειστικά στα δεδομένα τα οποία απαιτούνται για την εκτέλεση της εργασίας τους και όχι σε παραπάνω

ε) Αυθεντικοποίηση τερματικών Ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι οι χρήστες έχουν πρόσβαση αποκλειστικά στα δεδομένα τα οποία απαιτούνται μόνο από συγκεκριμένους σταθμούς εργασίας, όπως π.χ από συγκεκριμένες διευθύνσεις IP ή διευθύνσεις MAC.

14. Αρχεία καταγραφής

Η λειτουργία των αρχείων καταγραφής («log files») είναι ένα σημαντικό μέτρο ασφάλειας, καθώς επιτρέπει τον εντοπισμό των ενεργειών των χρηστών στις εφαρμογές, διευκολύνοντας έτσι την απόδοση ευθυνών (accountability) σε περίπτωση καταστροφής,

αλλοίωσης ή μη εξουσιοδοτημένης πρόσβασης στα δεδομένα.

Τα αρχεία καταγραφής πρέπει να είναι ενεργοποιημένα για ενέργειες εγγραφής, διόρθωσης και διαγραφής δεδομένων. Επίσης, πρέπει να γίνεται καταγραφή επιτυχημένων και αποτυχημένων προσπαθειών σύνδεσης των χρηστών τόσο σε επίπεδο λειτουργικού συστήματος όσο και σε επίπεδο εφαρμογών καθώς και στις επιμέρους βάσεις δεδομένων των εφαρμογών. Τα αρχεία καταγραφής πρέπει να συμπεριλαμβάνουν και τις ενέργειες των διαχειριστών των συστημάτων. Επίσης, πρέπει να καλύπτουν το μέγιστο δυνατό χρονικό διάστημα επεξεργασίας δεδομένων. Η πρόσβαση στα αρχεία καταγραφής πρέπει επίσης να καταγράφεται. Τα αρχεία καταγραφής πρέπει να επιβλέπονται ανά τακτά διαστήματα από αρμόδιο υπάλληλο του υπεύθυνου επεξεργασίας (π.χ. διαχειριστή ή/και υπεύθυνο ασφαλείας) για τυχόν ανίχνευση και αναγνώριση αθέμιτων ενεργειών, ενώ επίσης πρέπει να διασφαλίζεται η ακεραιότητά τους. Δεν θα πρέπει να υφίσταται δυνατότητα διαγραφής και αλλοίωσης των αρχείων καταγραφής. Θα πρέπει να υπάρχει δυνατότητα αυτόματης επίβλεψης των αρχείων καταγραφής.

Θα πρέπει να γίνεται καταγραφή ενεργειών ανάγνωσης δεδομένων (π.χ. εντολή «select» σε επίπεδο βάσης δεδομένων) και αλλαγών παραμετροποίησης των εφαρμογών, καθώς και καταγραφή των εντολών για εκτύπωση. Να δίνεται επίσης η δυνατότητα για προκαθορισμό ορισμένων κρίσιμων γεγονότων (events) η καταγραφή των οποίων θα επιβλέπεται άμεσα από τους διαχειριστές των συστημάτων.

15. Αντίγραφα ασφαλείας

Η τήρηση αντιγράφων ασφαλείας («back-up») είναι βασικό μέτρο για την εξασφάλιση της διαθεσιμότητας του πληροφοριακού συστήματος και των εφαρμογών σε περιπτώσεις εκτάκτων περιστατικών ασφαλείας και απώλειας ή καταστροφής δεδομένων. Η εφαρμογή συγκεκριμένης πολιτικής λήψης των αντιγράφων ασφαλείας συμβάλει σημαντικά στη ορθή εξαγωγή και αποθήκευσή τους.

α) Ο υπεύθυνος επεξεργασίας οφείλει να υιοθετήσει συγκεκριμένη πολιτική λήψης

αντιγράφων ασφαλείας, η οποία πρέπει να περιλαμβάνει χρόνους λήψης των αντιγράφων, μέτρα για την ασφαλή αποθήκευσή τους, καθώς και μέτρα για τον έλεγχο της ορθής εξαγωγής τους (περιοδικός έλεγχος ακεραιότητας/αξιοπιστίας των αντιγράφων που λαμβάνονται). Τα αντίγραφα ασφαλείας μπορεί να περιέχουν είτε τις ημερήσιες αλλαγές στις οποίες υπόκεινται τα δεδομένα είτε τα αυτούσια δεδομένα. Επίσης, πρέπει να οριστεί ο υπάλληλος που είναι υπεύθυνος για την εφαρμογή της πολιτικής λήψης αντιγράφων (στην περίπτωση που αυτός είναι διαφορετικός από τον υπεύθυνο ασφαλείας).

β) Τα αντίγραφα ασφαλείας πρέπει να αποθηκεύονται σε ασφαλή χώρο, σε διαφορετική τοποθεσία από τον τόπο λήψης, και να φέρουν κατάλληλη σήμανση. Για παράδειγμα μπορεί να είναι επισημασμένη η ημερομηνία λήψης των δεδομένων, το πεδίο λήψης των δεδομένων (εφαρμογή-ές, λειτουργικό σύστημα, δεδομένα δικτύου (fileserver) κτλ), το είδος του αντιγράφου (differential/incremental, full), η περιοδικότητα λήψης του κάθε αντιγράφου (ημερήσιο, εβδομαδιαίο, μηνιαίο, ετήσιο), καθώς και ο αριθμός των συνολικών αντιγράφων.

16. Ασφάλεια επικοινωνιών

Η ασφάλεια των επικοινωνιών είναι θεμελιώδες μέτρο για την προστασία των προσωπικών δεδομένων όταν αυτά διακινούνται μέσω δικτύου, όπως αυτό του πληροφοριακού συστήματος ενός νοσοκομείου, καθώς και κατά τη διασύνδεση τερματικών του εσωτερικού δικτύου του νοσοκομείου με μη ασφαλή δίκτυα, όπως το διαδίκτυο.

α) Σύνδεση με διαδίκτυο: Τερματικά και εξυπηρετητές που χρησιμοποιούνται κυρίως για την επεξεργασία των προσωπικών δεδομένων των ασθενών δεν πρέπει να συνδέονται στο διαδίκτυο.

β) Απομακρυσμένη πρόσβαση: Ο υπεύθυνος επεξεργασίας οφείλει κατά κανόνα να μην επιτρέπει την απομακρυσμένη πρόσβαση στελεχών του σε πόρους του συστήματος που περιέχουν προσωπικά δεδομένα ασθενών. Στην περίπτωση που αυτό είναι απολύτως απαραίτητο θα πρέπει να επιτρέπεται μόνο για συγκεκριμένα εξουσιοδοτημένα πρόσωπα

και να δικαιολογείται επαρκώς. Σε περίπτωση που απαιτείται απομακρυσμένη πρόσβαση σε συστήματα (π.χ. από συγκεκριμένα εξουσιοδοτημένα πρόσωπα ή από εταιρείες συντήρησης), ο υπεύθυνος επεξεργασίας πρέπει να ορίσει συγκεκριμένη διαδικασία διαχείρισης των απομακρυσμένων προσβάσεων. Ειδικότερα, κατ' ελάχιστον η απομακρυσμένη πρόσβαση πρέπει να γίνεται με την εποπτεία και έλεγχο του υπεύθυνου επεξεργασίας (π.χ. των διαχειριστών ή/και του υπεύθυνου ασφαλείας) με χρήση ειδικού κωδικού χρήστη και να καταγράφεται επαρκώς.

γ) Ασύρματη πρόσβαση: Η ασύρματη πρόσβαση πρέπει να είναι εξουσιοδοτημένη για συγκεκριμένους χρήστες και υπολογιστές με βάση τις ανάγκες του υπευθύνου επεξεργασίας. Η πρόσβαση πρέπει να προστατεύεται από κατάλληλους και αξιόπιστους αλγόριθμους κρυπτογράφησης.

δ) Κρυπτογράφηση: Ο υπεύθυνος επεξεργασίας πρέπει να εξασφαλίζει ότι η επικοινωνία γίνεται μέσω επαρκώς ασφαλούς καναλιού επικοινωνίας (π.χ. TLS ή VPN).

ε) Ο υπεύθυνος επεξεργασίας πρέπει να εξασφαλίζει επαρκή έλεγχο των συνδεόμενων στο δίκτυο συσκευών μέσω κατάλληλης παραμετροποίησης του δικτυακού εξοπλισμού (π.χ. MAC filtering).

17. Διαμόρφωση περιβάλλοντος υπολογιστών

Η διαμόρφωση υπολογιστών είναι σημαντικό μέτρο ασφαλείας, καθώς επιτρέπει τον έλεγχο των λειτουργιών του κάθε τερματικού του δικτύου, αποτρέποντας κατά τον τρόπο αυτό μη εξουσιοδοτημένες ενέργειες χρηστών (όπως π.χ. απενεργοποίηση αντιβιοτικών προγραμμάτων ή ανεξέλεγκτη εγκατάσταση λογισμικού), οι οποίες θα μπορούσαν να οδηγήσουν σε απώλεια, καταστροφή ή μη εξουσιοδοτημένη διάδοση προσωπικών δεδομένων.

α) Αντι-ιϊκά: Ο υπεύθυνος επεξεργασίας πρέπει να εξασφαλίζει προστασία από κακόβουλο λογισμικό όλων των υπολογιστών (τόσο των προσωπικών υπολογιστών των υπαλλήλων όσο και των εξυπηρετητών) μέσω των οποίων γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα με αντι-ιϊκά προγράμματα (antivirus). Τα προγράμματα θα πρέπει να είναι ενημερωμένα με τους ορισμούς των ιών τουλάχιστον

ανά ημέρα και με τις ενημερώσεις των μηχανών εβδομαδιαία. Δεν θα πρέπει να υπάρχει δυνατότητα απενεργοποίησης των αντι-ιϊκών προγραμμάτων από τους χρήστες.

β) Αποσπώμενα μέσα: Τερματικά και εξυπηρετητές που χρησιμοποιούνται κυρίως για την επεξεργασία των προσωπικών δεδομένων των ασθενών (π.χ. στο τμήμα των εργαστηρίων ή των εξωτερικών ιατρείων) δεν πρέπει να επιτρέπουν την εξαγωγή δεδομένων με τη χρήση αποσπώμενων μέσων (π.χ. USB, CD/DVD).

γ) Ο υπεύθυνος επεξεργασίας πρέπει να διαθέτει συγκεκριμένη πολιτική για τη χρήση των φορητών υπολογιστών ή άλλων φορητών/αποσπώμενων μέσων εκτός των εγκαταστάσεών του όταν τα τελευταία περιέχουν προσωπικά δεδομένα ασθενών. Η εν λόγω πολιτική πρέπει να περιλαμβάνει τουλάχιστον καταγραφή της ημέρας και ώρας εξόδου του φορητού υπολογιστή, καθώς και του ατόμου που τον χρησιμοποιεί. Επίσης, η χρήση φορητών υπολογιστών με προσωπικά δεδομένα εκτός των εγκαταστάσεων του υπεύθυνου επεξεργασίας πρέπει να επιτρέπεται σε συγκεκριμένα εξουσιοδοτημένα άτομα και να δικαιολογείται επαρκώς.

δ) Κρυπτογράφηση φορητών μέσων: Στην περίπτωση που χρησιμοποιούνται φορητά μέσα (π.χ. φορητοί υπολογιστές, USB, CD/DVD) που περιέχουν προσωπικά δεδομένα εκτός των εγκαταστάσεων του υπευθύνου επεξεργασίας, τα δεδομένα πρέπει να είναι κρυπτογραφημένα.

ε) Εγκατάσταση προγράμματος: Η εγκατάσταση προγραμμάτων στα προσωπικά τερματικά των υπαλλήλων πρέπει να γίνεται μετά από κατάλληλη εξουσιοδότηση του υπεύθυνου επεξεργασίας από αρμόδιο υπάλληλό του (π.χ. διαχειριστή). Ο υπεύθυνος επεξεργασίας πρέπει να εξασφαλίζει τον περιοδικό έλεγχο του εγκατεστημένου λογισμικού και τον εντοπισμό προγραμμάτων που έχουν εγκατασταθεί εκτός των εγκεκριμένων διαδικασιών.

στ) Όταν ένας χρήστης απομακρύνεται από το σταθμό εργασίας του και αυτός παραμένει σε λειτουργία, πρέπει να ενεργοποιείται η προφύλαξη οθόνης (screen saver) η οποία θα απενεργοποιείται μόνο με χρήση συνθηματικού. Εξάλλου, σε επίπεδο εφαρμογής, μετά από ορισμένο χρόνο αδράνειας (π.χ. 30 λεπτά), θα πρέπει να τερματίζεται η συνεδρία (session time-out) χρήσης της εφαρμογής. Σε κάθε περίπτωση, η συνεδρία θα πρέπει να τερματίζεται με την λήξη της εργασίας του συγκεκριμένου χρήστη

στον σταθμό εργασίας.

ζ) Τα αντι-ιϊκά προγράμματα (antivirus) θα πρέπει να αναζητούν εκτός από τους ορισμούς (τις υπογραφές) των ιών, και τα χαρακτηριστικά συμπεριφοράς (heuristics) των προγραμμάτων που ανιχνεύονται.