ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 24-11-2014

Αριθ. Πρωτ.: Γ/ΕΞ/7173/24-11-2014

Α Π Ο Φ Α Σ Η 176/2014

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε στην έδρα της την Τρίτη 14.10.2014 και ώρα 10:00, εξ αναβολής από τις συνεδριάσεις της 23ης.07.2014 και 30ης.07.2014, μετά από πρόσκληση του Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Πρόεδρος της Αρχής, Πέτρος Χριστόφορος και τα τακτικά μέλη της Αρχής Λεωνίδας Κοτσαλής, Αναστάσιος-Ιωάννης Μεταξάς, Δημήτριος Μπριόλας, Αντώνιος Συμβώνης, Κωνσταντίνος Χριστοδούλου και Πέτρος Τσαντίλας, ως εισηγητής. Στη συνεδρίαση παρέστη ακόμα το αναπληρωματικό μέλος της Αρχής, Παναγιώτης Ροντογιάννης, ως εισηγητής. Παρούσες χωρίς δικαίωμα ψήφου ήταν οι Χαρίκλεια Λάτσιου, νομικός ελεγκτής-δικηγόρος και Γεωργία Παναγοπούλου, πληροφορικός-ελεγκτής, ως βοηθοί εισηγήτριες. Ως βοηθός εισηγήτρια είχε οριστεί η Ζωή Καρδασιάδου, η οποία λόγω κωλύματος δεν παρέστη στη συνεδρίαση αυτή (της 14ης .10.2014). Παρέστη, επίσης, η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας, με εντολή του Προέδρου.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Με το υπ' αρ. πρωτ. …/..-..-2013 (υπ' αρ. πρωτ. ΑΠΔΠΧ Γ/ΕΙΣ/7532/25.11.2013) έγγραφο το Νοσοκομείο Λαϊκό διαβιβάζει το υπ' αρ. πρωτ. …/..-..-2013 έγγραφο του Τμήματος Ανοσολογίας – Ιστοσυμβατότητας του Νοσοκομείου και ζητεί από την Αρχή: «*όπως μας απαντήσε[ι] σχετικά με το ερώτημα της τελευταίας παραγράφου, το οποίο αναφέρεται σε χορήγηση στοιχείων σχετικών με Ευαίσθητα Προσωπικά Δεδομένα μέσω ηλεκτρονικού ταχυδρομείου, καθώς και τα κριτήρια που θα πρέπει να πληρούνται σε τέτοια περίπτωση*». Συγκεκριμένα, η Δ/ντρια του Τμήματος Ανοσολογίας –

Ιστοσυμβατότητας του Νοσοκομείου με το από ..-..-2013 έγγραφό της προς τη Διοίκηση του Νοσοκομείου, αναφερόμενη στα προβλήματα εφαρμογής του νέου πληροφοριακού συστήματος της εταιρείας CCS στο Τμήμα αυτό, καταλήγει στο ακόλουθο ερώτημα: «*Επίσης, επανέρχομαι εκ νέου στο Αριθμ. Πρωτ. …/..-..-2013 αίτημά μας για την εγκατάσταση της δυνατότητας αποστολής των αποτελεσμάτων των εξωτερικών ασθενών μέσω ηλεκτρονικού ταχυδρομείου σε μη επεξεργάσιμη μορφή, καθώς το Τμήμα στερείται γραμματέως από το 2011*».

Η Αρχή, κατά την εξέταση της υπόθεσης, κάλεσε με το υπ' αρ. πρωτ. Γ/ΕΞ/2973/12.05.2014 έγγραφο το Νοσοκομείο Λαϊκό να παράσχει συγκεκριμένες διευκρινίσεις. Σε απάντηση του εγγράφου αυτού, το Νοσοκομείο Λαϊκό απέστειλε το υπ' αρ. πρωτ. …/..-..-2014 (υπ' αρ. πρωτ. ΑΠΔΠΧ Γ/ΕΙΣ/3696/12.06.2014) έγγραφο, διευκρινίζοντας, μεταξύ άλλων, ότι το ερώτημα της αποστολής ιατρικών αποτελεσμάτων των ασθενών μέσω ηλεκτρονικού ταχυδρομείου αφορά, προς το παρόν, μόνο στο Τμήμα Ανοσολογίας – Ιστοσυμβατότητας και όχι και άλλα Τμήματα του συγκεκριμένου Νοσοκομείου. Ακολούθως, η Αρχή με το υπ' αρ. πρωτ. Γ/ΕΞ/3422/30.05.2014 έγγραφο κάλεσε το Νοσοκομείο Λαϊκό, όπως νομίμως εκπροσωπείται, να παραστεί στη συνεδρίαση της Αρχής την 18^{η}.06.2014 προκειμένου να συζητηθεί το υποβληθέν στην Αρχή ερώτημα. Στη συνεδρίαση της Αρχής την 18^{η}.06.2014 παρέστησαν οι Α, και Β, μέλη της Επιτροπής Ασφαλείας του Νοσοκομείου. Κατά τη συνεδρίαση αυτή, η Αρχή αποφάσισε να διακόψει τη συνεδρίαση και να ζητήσει την εκπροσώπηση του Νοσοκομείου στο υψηλότερο δυνατό επίπεδο ενώπιον της Αρχής σε νέα συνεδρίαση την 02^{η}.07.2014, προκειμένου να εξετασθεί το υποβληθέν ερώτημα.

Στη συνεδρίαση της Αρχής την 02^{η}.07.2014 παρέστησαν οι Γ, Δ, Ε, Α, και Β, μέλη της Επιτροπής Ασφαλείας του Νοσοκομείου. Κατά τη συνεδρίαση αυτή η Αρχή, αφού άκουσε τις απόψεις των εκπροσώπων του Νοσοκομείου για το υποβληθέν ερώτημα, έθεσε προθεσμία ως τις 16.07.2014 για την υποβολή έγγραφου υπομνήματος. Παράλληλα, η Αρχή με το υπ' αρ. πρωτ. Γ/ΕΞ/4254/04.07.2014 έγγραφο, κατόπιν αιτήματος του Νοσοκομείου, υπέβαλε εγγράφως συγκεκριμένα ερωτήματα που ανέκυψαν κατά τη συνεδρίαση της 02^{ης}.07.2014. Σε απάντηση του εγγράφου αυτού της Αρχής, το Νοσοκομείο Λαϊκό με το υπ' αρ. πρωτ. …/..-..-2014 (υπ' αρ. πρωτ. ΑΠΔΠΧ Γ/ΕΙΣ/4472/16.07.2014) έγγραφο ενημέρωσε την Αρχή, μεταξύ άλλων, ότι: «*Έχοντας υπόψη όσα διαλαμβάνονται στις παρ. 1 έως και 24 του άρθρου 14 του Ν.2672/98 (Διακίνηση εγγράφων με ηλεκτρονικά μέσα, τηλεομοιοτυπία – ηλεκτρονικό ταχυδρομείο), καθώς επίσης και στα άρθρα 4, 6, 7, 8, 18, 21, 30 κ.λ.π. του Ν.3979/2011 (για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις) και την υπ'*

αριθμ. ΥΑΠ/Φ40.4/1/989 (ΦΕΚ Β΄ αρ. φυλ. 1301 της 124/2012 (άρθρο 1 παρ. 2,3) φρονούμε ότι το ισχύον δίκαιο επιτρέπει τη χρήση ηλεκτρονικού ταχυδρομείου για την αποστολή αποτελεσμάτων ιατρικών εξετάσεων με εξαίρεση την παρ. 6 του άρθρου 14 του Ν.2672/198 δηλαδή "τα έγγραφα τα οποία περιέχουν ευαίσθητα δεδομένα προσωπικού χαρακτήρα, σύμφωνα με τις διατάξεις της κείμενης νομοθεσίας για την προστασία ατόμων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα". Αλλά και σ' αυτή όμως την περίπτωση φρονούμε ότι δεν υφίσταται κανένα απολύτως θέμα εφ' όσον διασφαλίζεται η συγκατάθεση του ενδιαφερομένου στον οποίον αφορούν οι ιατρικές εξετάσεις προς εξυπηρέτηση και διευκόλυνση του οποίου αποστέλλονται αυτές (…) Σε κάθε περίπτωση το Νοσοκομείο είναι σε θέση να εφαρμόσει τις οποιεσδήποτε υποδείξεις και να χρησιμοποιήσει τα οποιαδήποτε ενδεδειγμένα σύγχρονα τεχνικά μέσα προς μεγαλύτερη εξασφάλιση και διαφύλαξη των προσωπικών δεδομένων των ασθενών κατά την αποστολή σ' αυτούς των ιατρικών τους εξετάσεως μέσω (ηλεκτρονικού ταχυδρομείου) (…)».

Η Αρχή, μετά από εξέταση των στοιχείων του φακέλου, αφού έγινε μνεία στα διαμειφθέντα κατά τις συνεδριάσεις των 18ης.06.2014 και 02ας.07.2014, άκουσε τους εισηγητές και τις βοηθούς εισηγητών, οι οποίες στη συνέχεια αποχώρησαν και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΤΗΚΕ ΣΥΜΦ ΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Επειδή, το άρθρο 12 του ν.2472/1997 προβλέπει: «*1. Καθένας έχει δικαίωμα να γνωρίζει εάν δεδομένα προσωπικού χαρακτήρα που τον αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Προς τούτο, ο υπεύθυνος επεξεργασίας, έχει υποχρέωση να του απαντήσει εγγράφως. 2. Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή, τις ακόλουθες πληροφορίες: α) Όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, καθώς και την προέλευσή τους. β) Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών. γ) Την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση ή πληροφόρησή του. δ) Τη λογική της αυτοματοποιημένης επεξεργασίας. Το δικαίωμα πρόσβασης μπορεί να ασκείται από το υποκείμενο των δεδομένων και με τη συνδρομή ειδικού. ε) κατά περίπτωση, τη διόρθωση, τη διαγραφή ή τη δέσμευση (κλείδωμα) των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις του παρόντος νόμου, ιδίως λόγω του ελλιπούς ή ανακριβούς χαρακτήρα των δεδομένων, και στ) την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδομένα, κάθε διόρθωσης, διαγραφής ή*

δέσμευσης (κλειδώματος) που διενεργείται σύμφωνα με την περίπτωση ε, εφόσον τούτο δεν είναι αδύνατον ή δεν προϋποθέτει δυσανάλογες προσπάθειες. 3. Το δικαίωμα της προηγούμενης παραγράφου και τα δικαιώματα του άρθρου 13 ασκούνται με την υποβολή της σχετικής αίτησης στον υπεύθυνο της επεξεργασίας και ταυτόχρονη καταβολή χρηματικού ποσού, το ύψος του οποίου, ο τρόπος καταβολής του και κάθε άλλο συναφές ζήτημα ρυθμίζονται με απόφαση της Αρχής. Το ποσό αυτό επιστρέφεται στον αιτούντα εάν το αίτημα διόρθωσης ή διαγραφής των δεδομένων κριθεί βάσιμο είτε από τον υπεύθυνο της επεξεργασίας είτε από την Αρχή, σε περίπτωση προσφυγής του σ' αυτήν. Ο υπεύθυνος έχει υποχρέωση στην περίπτωση αυτή να χορηγήσει στον αιτούντα, χωρίς καθυστέρηση δωρεάν και σε γλώσσα κατανοητή, αντίγραφο του διορθωμένου μέρους της επεξεργασίας που τον αφορά». Το άρθρο 10 του ν.2472/1997 καθιερώνει δύο θεμελιώδεις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων και καθορίζουν τη νομιμότητά της: την αρχή του απορρήτου και της ασφάλειας της επεξεργασίας. Βάσει των αρχών αυτών, ο υπεύθυνος επεξεργασίας βαρύνεται, μεταξύ άλλων, με την λήψη των κατάλληλων οργανωτικών και τεχνικών μέτρων για την προστασία των προσωπικών δεδομένων από τυχαία καταστροφή, τυχαία απώλεια, και από κάθε αθέμιτη επεξεργασία. Η παράβαση δε των υποχρεώσεων που καθιερώνονται με το άρθρο 10 του ν.2472/1997 επισύρει διοικητικές και ποινικές κυρώσεις και ιδρύει, υπό προϋποθέσεις, αστική ευθύνη του υπευθύνου επεξεργασίας, σύμφωνα με τα οριζόμενα στις διατάξεις των άρθρων 21, 22 και 23 του ν.2472/1997. Επιπλέον, το άρθρο 14 του ν.3418/2005 προβλέπει ότι: «*1. Ο ιατρός υποχρεούται να τηρεί ιατρικό αρχείο, σε ηλεκτρονική ή μη μορφή, το οποίο περιέχει δεδομένα που συνδέονται αρρήκτως ή αιτιωδώς με την ασθένεια ή την υγεία των ασθενών του. Για την τήρηση του αρχείου αυτού και την επεξεργασία των δεδομένων του εφαρμόζονται οι διατάξεις του ν.2472/1997 (ΦΕΚ 50 Α΄). (…). 3. Οι κλινικές και τα νοσοκομεία τηρούν στα ιατρικά τους αρχεία και τα αποτελέσματα όλων των κλινικών και παρακλινικών εξετάσεων. (…) 7. Ο ασθενής έχει δικαίωμα πρόσβασης στα ιατρικά αρχεία, καθώς και λήψης αντιγράφων του φακέλου του (…)*». Από το συνδυασμό των ανωτέρω διατάξεων των νόμων 2472/1997 και 3418/2005 προκύπτει ότι ο ασθενής, ως υποκείμενο των δεδομένων, έχει δικαίωμα πρόσβασης στον ιατρικό του φάκελο και λήψης αντιγράφων αυτού, το δε νοσηλευτικό ίδρυμα, ως υπεύθυνος επεξεργασίας, οφείλει να ικανοποιήσει το δικαίωμά του αυτό, λαμβάνοντας τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την προστασία των προσωπικών δεδομένων, μεταξύ άλλων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, απαγορευμένη διάδοση και από κάθε μορφής αθέμιτη επεξεργασία.

2. Επειδή, περαιτέρω, το άρθρο 14 του ν. 2672/1998 (ΦΕΚ Α΄ 290), όπως τροποποιήθηκε και

ισχύει, προβλέπει ότι: «1. *Επιτρέπεται η διακίνηση εγγράφων μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των οργανισμών τοπικής αυτοδιοίκησης ή μεταξύ αυτών και των ενδιαφερόμενων φυσικών προσώπων, νομικών προσώπων ιδιωτικού δικαίου και ενώσεων προσώπων με τηλεμοιοτυπία και ηλεκτρονικό ταχυδρομείο* (…) 4. *Μεταξύ των υπηρεσιών της παραγράφου 1, διακινούνται με ηλεκτρονικό ταχυδρομείο, κατά τις διατάξεις του παρόντος άρθρου, μηνύματα που έχουν ως περιεχόμενο γνωμοδοτήσεις, ερωτήματα, αιτήσεις, απαντήσεις, εγκυκλίους, οδηγίες, εκθέσεις, μελέτες, πρακτικά, στατιστικά στοιχεία, υπηρεσιακά σημειώματα και έγγραφες εισηγήσεις. Κατά τον παραπάνω τρόπο διακινούνται μεταξύ των υπηρεσιών αυτών και των φυσικών και νομικών προσώπων ιδιωτικού δικαίου μηνύματα που έχουν ως περιεχόμενο αιτήσεις παροχής πληροφοριών και σχετικές απαντήσεις. 5. Για τη διακίνηση εγγράφων με τηλεομοιοτυπία ή μηνυμάτων με ηλεκτρονικό ταχυδρομείο προς φυσικά πρόσωπα, νομικά πρόσωπα ιδιωτικού δικαίου ή ενώσεις φυσικών προσώπων απαιτείται η συγκατάθεσή τους. Τα φυσικά ή νομικά πρόσωπα ιδιωτικού δικαίου μπορούν να δηλώνουν της προτίμησή τους ως προς το μέσο της απάντησης. Σε διαφορετική περίπτωση τεκμαίρεται η συγκατάθεσή τους για τη διακίνηση της απάντησης με το ίδιο μέσο. 6. Από τις διατάξεις των παραγράφων 3 και 4 εξαιρούνται: (…) β. Τα έγγραφα τα οποία περιέχουν ευαίσθητα δεδομένα προσωπικού χαρακτήρα, σύμφωνα με τις διατάξεις της κείμενης νομοθεσίας για την προστασία ατόμων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (…)*». Από τον συνδυασμό των ανωτέρω διατάξεων του άρθρου 14 του ν.2672/1998 η Αρχή δέχεται, κατά πλειοψηφία, ότι η ικανοποίηση του δικαιώματος πρόσβασης του ασθενούς στα ιατρικά αρχεία νοσηλευτικού ιδρύματος με την αποστολή αποτελεσμάτων κλινικών ή παρακλινικών εξετάσεων μέσω ηλεκτρονικού ταχυδρομείου από νοσηλευτικό ίδρυμα Ν.Π.Δ.Δ., επιτρέπεται, όταν ο ασθενής, ως υποκείμενο των δεδομένων έχει εγγράφως ζητήσει ρητά η αποστολή των δεδομένων αυτών της υγείας του να πραγματοποιηθεί με ηλεκτρονικό ταχυδρομείο. Τούτο δε διότι η συγκατάθεση του υποκειμένου των δεδομένων είναι ισχυρή και όταν αναφέρεται σε ευαίσθητα δεδομένα. Άλλωστε το γράμμα της διατάξεως της παραγράφου 6 του άρθρου 14 δεν αποκλείει την εφαρμογή της παραγράφου 4 όταν υπάρχει συγκατάθεση του υποκειμένου, θέμα που ρυθμίζεται ρητά στην παράγραφο 5 του άρθρου 14 του ν.2672/1998. Τα ανωτέρω τελούν υπό την προϋπόθεση ότι τηρούνται τα κατάλληλα οργανωτικά και τεχνικά μέτρα ασφάλειας για την επεξεργασία των προσωπικών δεδομένων, σύμφωνα με τα οριζόμενα στο άρθρο 10 παρ. 3 του ν.2472/1997, τα οποία, ως προς τα θέματα παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης, ρυθμίζονται πλέον ειδικότερα και στο νόμο 3979/2011 και το Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Αντίθετα, κατά την άποψη δύο μελών της Αρχής, η αποστολή αποτελεσμάτων ιατρικών εξετάσεων

ασθενών με ηλεκτρονικό ταχυδρομείο από νοσηλευτικό ίδρυμα Ν.Π.Δ.Δ. ακόμα και με τη συγκατάθεση των ασθενών απαγορεύεται, καθώς κατισχύει η παράγραφος 6 του άρθρου 14 του νόμου 2672/1998, που απαγορεύει γενικά την αποστολή με ηλεκτρονικό ταχυδρομείο εγγράφων που περιέχουν ευαίσθητα δεδομένα προσωπικού χαρακτήρα.

3. Επειδή, ειδικότερα, ο νόμος 3979/2011 (ΦΕΚ Α΄ 138) προβλέπει ότι στις υπηρεσίες ηλεκτρονικής διακυβέρνησης περιλαμβάνονται οι υπηρεσίες που συνίστανται στην παραγωγή, διακίνηση και διαχείριση πληροφοριών δεδομένων και ηλεκτρονικών εγγράφων και στην παροχή υπηρεσιών από φορείς του δημόσιου τομέα ή στην πραγματοποίηση συναλλαγών με αυτούς του φορείς με χρήση ΤΠΕ (άρθρο 3). Το άρθρο 7 του νόμου αυτού ορίζει ότι: «*1. Οι φορείς του δημοσίου τομέα παρέχουν υπηρεσίες ηλεκτρονικής διακυβέρνησης με σεβασμό του δικαιώματος προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικότητας των φυσικών προσώπων. 2. Κατά το σχεδιασμό, διαμόρφωση και προμήθεια πληροφοριακών συστημάτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης γίνεται αξιολόγηση των επιπτώσεών τους στην ιδιωτικότητα και στην προστασία των δεδομένων προσωπικού χαρακτήρα (…)*». Ακολούθως, το άρθρο 21 προβλέπει ότι: «*1. Με την επιφύλαξη ειδικών ρυθμίσεων που καθιστούν υποχρεωτική τη χρήση ΤΠΕ για την επικοινωνία και τη συναλλαγή με φορέα του δημόσιου τομέα, ο φορέας του δημόσιου τομέα μπορεί να χρησιμοποιεί ηλεκτρονικό τρόπο επικοινωνίας με φυσικά πρόσωπα ή Ν.Π.Ι.Δ. και παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης σε αυτά, εφόσον τα πρόσωπα αυτά έχουν ζητήσει τη χρήση του τρόπου αυτού ή έχουν δώσει τη ρητή συγκατάθεσή τους. Η αίτηση και η παροχή της συγκατάθεσης, καθώς και η ανάκλησή της μπορούν να διαβιβάζονται και με ηλεκτρονικό τρόπο, εφόσον τηρούνται οι προϋποθέσεις της ταυτοποίησης και επιβεβαίωσης ταυτότητας (αυθεντικοποίησης). 2. Οι φορείς του δημόσιου τομέα επικοινωνούν και συναλλάσσονται με φυσικά πρόσωπα και Ν.Π.Ι.Δ. και εν γένει παρέχουν υπηρεσίες ηλεκτρονικής διακυβέρνησης σε αυτά, τηρώντας τις προϋποθέσεις και τους όρους ασφαλείας που περιέχονται στο προβλεπόμενο στο άρθρο 27 του ν.3731/2008 Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης ή στην πολιτική ασφαλείας του εκάστοτε φορέα του δημοσίου τομέα*». Εν συνεχεία, το άρθρο 25 ορίζει στην παράγραφο 1: «*Οι φορείς του δημόσιου τομέα διακινούν ή ανταλλάσσουν με χρήση ΤΠΕ έγγραφα και δεδομένα στο πλαίσιο της άσκησης των αρμοδιοτήτων που τους έχουν ανατεθεί και για την εκπλήρωση αυτών, υπό την προϋπόθεση ότι τηρούνται οι όροι ασφάλειας στο επίπεδο που κάθε φορά επιβάλλεται από τη φύση των διακινούμενων εγγράφων και επιβεβαιώνεται η ταυτότητα (αυθεντικοποίηση) των δημόσιων λειτουργών και υπαλλήλων. Οι όροι ασφάλειας που πρέπει να τηρούνται για τη διακίνηση των εγγράφων μεταξύ φορέων του δημόσιου*

τομέα, καθώς και άλλο σχετικό θέμα καθορίζονται με απόφαση του Υπουργού Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης». Ακολούθως, το άρθρο 30 παρ. 1 προβλέπει ότι: «*Η ταυτοποίηση και αυθεντικοποίηση των φυσικών προσώπων που επικοινωνούν και συναλλάσσονται με φορείς του δημοσίου τομέα είναι υποχρεωτική: α) εφόσον η επικοινωνία ή η συναλλαγή: (…) γγ) αφορά την έκδοση, αναπαραγωγή ή κοινοποίηση πράξεων, βεβαιώσεων, πιστοποιητικών και εν γένει εγγράφων, τα οποία περιέχουν ή σχετίζονται με δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων που συναλλάσσονται με τη διοίκηση (…)*». Συνεπώς, σύμφωνα με τις προαναφερόμενες διατάξεις του ν. 3979/2011 η αποστολή αποτελεσμάτων ιατρικών εξετάσεων ασθενών από νοσηλευτικό ίδρυμα Ν.Π.Δ.Δ, όπως το Νοσοκομείο Λαϊκό, μέσω ηλεκτρονικού ταχυδρομείου επιτρέπεται, εφόσον οι ασθενείς, ως υποκείμενα των δεδομένων, έχουν δώσει την προηγούμενη ρητή συγκατάθεσή τους για το συγκεκριμένο τρόπο της ικανοποίησης του δικαιώματος πρόσβασης, με την προϋπόθεση ότι εκπληρώνεται η υποχρέωση της ταυτοποίησης και επιβεβαίωσης (αυθεντικοποίησης) τόσο των φυσικών προσώπων (ασθενών, ως υποκειμένων των δεδομένων) όσο και του συγκεκριμένου νοσηλευτικού ιδρύματος (Νοσοκομείο Λαϊκό), και εφόσον τηρούνται οι προϋποθέσεις και οι όροι ασφάλειας που περιέχονται στο προβλεπόμενο από το άρθρο 27 του ν. 3731/2008 Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης.

4. Συναφώς, κατ' εξουσιοδότηση των άρθρων 27 του ν.3731/2008 και 21 παρ. 2 του ν.3979/2011 εκδόθηκε η υπ' αρ. ΥΑΠ/Φ.40.4/1/989 (ΦΕΚ Β΄ 1301/12.04.2012) υπουργική απόφαση του Υφυπουργού Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης, με τίτλο «Κύρωση Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης», στην οποία προβλέπονται οι προϋποθέσεις ταυτοποίησης και επιβεβαίωσης (αυθεντικοποίησης) ανάλογα με την κατηγορία των δεδομένων που αξιοποιούν (προσωπικά, ευαίσθητα και οικονομικά), αλλά και τις πιθανές επιπτώσεις που μπορεί να προκληθούν σε περίπτωση μη ορθής λειτουργίας ή διαχείρισής τους. Ειδικότερα, προβλέπεται ότι στο Επίπεδο Εμπιστοσύνης 3 εντάσσονται υπηρεσίες που απαιτούν ανταλλαγή, είτε ευαίσθητων προσωπικών, είτε υπηρεσίες ηλεκτρονικής ολοκλήρωσης επιπέδου 4, όπου ο χρήστης πραγματοποιεί και τις οικονομικές συναλλαγές που απαιτούνται με ηλεκτρονικό τρόπο. Συνεπώς, οι επιπτώσεις που μπορεί να προκληθούν από κάποιο περιστατικό ασφάλειας είναι ιδιαίτερα σημαντικές και ως εκ τούτου είναι απαραίτητο να διασφαλιστεί υψηλός βαθμός εμπιστοσύνης για την ηλεκτρονική ταυτότητα ενός χρήστη. Περαιτέρω, στο Επίπεδο Αυθεντικοποίησης 2 προβλέπεται ότι σε αυτό το επίπεδο αυθεντικοποίησης απαιτείται υψηλή βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας μιας οντότητας, καθώς είναι εξαιρετικά κρίσιμο να εξασφαλιστεί ότι μόνο

εξουσιοδοτημένα πρόσωπα έχουν τη δυνατότητα πρόσβασης στις προσφερόμενες υπηρεσίες. Εδώ εντάσσονται οι ηλεκτρονικές υπηρεσίες που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα ή υποστηρίζουν τη διενέργεια οικονομικών συναλλαγών. Στη σύνοψη συσχετισμού Επιπέδων Εμπιστοσύνης και Αυθεντικοποίησης προβλέπεται ότι για το Επίπεδο Εμπιστοσύνης 3 απαιτείται Επίπεδο Αυθεντικοποίησης 2. Πρέπει πάντως να σημειωθεί ότι, στους κανόνες που έχουν τυποποιηθεί στο τέλος του παραρτήματος της υπουργικής αυτής απόφασης ορίζεται ότι στις υπηρεσίες που έχουν ενταχθεί στο Επίπεδο Εμπιστοσύνης 3 πρέπει να υιοθετηθεί επίπεδο Αυθεντικοποίησης τουλάχιστον 1, ενώ συνιστάται Επίπεδο Αυθεντικοποίησης 2, προβλέπεται δε να υιοθετηθεί και Επίπεδο Εγγραφής 3 (ΚΥ.10).

5. Η Αρχή, εξειδικεύοντας τα προαναφερόμενα επίπεδα εμπιστοσύνης και επίπεδα αυθεντικοποίησης, καθώς και τα επίπεδα εγγραφής που καθορίζονται στην προαναφερόμενη υπουργική απόφαση, κρίνει ότι κατ' εφαρμογή των ανωτέρω διατάξεων των νόμων 2472/1997, 2672/1998 και 3979/2011, προκειμένου τα αποτελέσματα ιατρικών εξετάσεων να αποστέλλονται από το Νοσοκομείο Λαϊκό με ασφαλή τρόπο μέσω ηλεκτρονικού ταχυδρομείου στους ασθενείς που έχουν ρητά συγκατατεθεί προς τούτο, θα πρέπει, ιδίως, να ακολουθούντα τα παρακάτω:

i) Ο ενδιαφερόμενος ασθενής θα πρέπει να υποβάλλει εγγράφως την αίτησή του για την αποστολή των ιατρικών αποτελεσμάτων του μέσω ηλεκτρονικού ταχυδρομείου, και να επιδεικνύει επίσημο έγγραφο (π.χ. ΑΔΤ) που να επιβεβαιώνει την ταυτότητά του.

ii) Συνίσταται η πραγματοποίηση επαλήθευσης της δηλωθείσας διεύθυνσης ηλεκτρονικού ταχυδρομείου, προς αποφυγή λανθασμένης καταχώρισης στο πληροφοριακό σύστημα του νοσηλευτικού ιδρύματος ή αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου σε λάθος παραλήπτη (βλ. ιδίως απόφαση Αρχής 164/2014, δημοσιευμένη στην ιστοσελίδα της).

iii) Τα ιατρικά αποτελέσματα των ασθενών που αποστέλλονται με ηλεκτρονικό ταχυδρομείο θα πρέπει να είναι κρυπτογραφημένα με χρήση διεθνώς αποδεκτών προτύπων αλγορίθμων κρυπτογράφησης, τα οποία μόνο ο παραλήπτης (ασθενής, ως υποκείμενο των δεδομένων) μπορεί να αποκρυπτογραφήσει. Ο ασθενής πρέπει να λαμβάνει από το νοσηλευτικό ίδρυμα ισχυρό συνθηματικό αποκρυπτογράφησης, με μέσο διαφορετικό του μηνύματος ηλεκτρονικού ταχυδρομείου (π.χ. SMS, έγγραφο).

iv) Η αποστολή των ιατρικών αποτελεσμάτων των ασθενών θα πρέπει να ανατίθεται από το νοσηλευτικό ίδρυμα σε συγκεκριμένους εξουσιοδοτημένους υπαλλήλους του νοσοκομείου, οι οποίοι πρέπει να δεσμεύονται εγγράφως σχετικά με την τήρηση της εχεμύθειας και της εμπιστευτικότητας

και να υπόκεινται σε κώδικα δεοντολογίας σχετικά με την προστασία των προσωπικών δεδομένων, ο οποίος πρέπει να φέρει την έγκριση της διοίκησης του υπευθύνου επεξεργασίας και να είναι δεσμευτικός για τους υπαλλήλους. Θα πρέπει να υπάρχουν κατάλληλοι μηχανισμοί για την αναγνώριση και αυθεντικοποίηση των υπαλλήλων αυτών. Στην περίπτωση που 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. Οι μηχανισμοί αυτοί σε συνδυασμό με τις κατάλληλες διαδικασίες διαχείρισης χρηστών, αποτελούν βασικό μέτρο προστασίας από μη εξουσιοδοτημένη πρόσβαση.

v) Τα αποστελλόμενα μηνύματα ηλεκτρονικού ταχυδρομείου θα πρέπει να τηρούνται στο νοσηλευτικό ίδρυμα, προκειμένου να διευκολύνεται η λογοδοσία (accountability), σε περίπτωση καταστροφής, αλλοίωσης ή μη εξουσιοδοτημένης πρόσβασης στα δεδομένα[1], καθώς και να διασφαλίζεται η ορθή εκπλήρωση της υποχρέωσης του νοσηλευτικού ιδρύματος για την ικανοποίηση του δικαιώματος πρόσβασης, μέσω της αποστολής ηλεκτρονικού ταχυδρομείου.

vi) Η διαμόρφωση των Η/Υ, μέσω των οποίων πραγματοποιείται η αποστολή των μηνυμάτων ηλεκτρονικού ταχυδρομείου, πρέπει να επιτρέπει τον έλεγχο των λειτουργιών τους, αποτρέποντας μη εξουσιοδοτημένες ενέργειες χρηστών οι οποίες θα μπορούσαν να οδηγήσουν σε απώλεια, καταστροφή ή μη εξουσιοδοτημένη επεξεργασία προσωπικών δεδομένων. Επιπλέον, στους Η/Υ πρέπει να εξασφαλίζεται προστασία από κακόβουλο λογισμικό με αντιϊκά προγράμματα (antivirus). Τα προγράμματα θα πρέπει να είναι ενημερωμένα με τους ορισμούς των ιών, τουλάχιστον ανά ημέρα και με τις ενημερώσεις των μηχανών ανά εβδομάδα. Δεν θα πρέπει να υπάρχει δυνατότητα απενεργοποίησης των αντιϊκών προγραμμάτων από τους χρήστες.

vii) Θα πρέπει να απαγορεύεται η εξαγωγή προσωπικών δεδομένων των ασθενών με τη χρήση αποσπώμενων μέσων (π.χ. USB, CD/DVD). Όταν ο εξουσιοδοτημένος υπάλληλος απομακρύνεται από τον Η/Υ του και αυτός παραμένει σε λειτουργία, πρέπει να ενεργοποιείται η προφύλαξη οθόνης (screen saver) η οποία θα απενεργοποιείται μόνο με χρήση συνθηματικού.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

[1] Πρόκειται, ιδίως, για περιστατικά παραβίασης προσωπικών δεδομένων, βλ. άρθρο 2 στοιχ. 11 ν.3471/2006, όπως προστέθηκε με το άρθρο 168 παρ. 1 στοιχ. δ΄ του ν.4070/2012, βλ., ιδίως, αποφάσεις της Αρχής 87/2011, 59/2012, 98/2013, δημοσιευμένες στην ιστοσελίδα της.

Η Αρχή αποφαίνεται ότι:

1) Η αποστολή αποτελεσμάτων ιατρικών εξετάσεων ασθενών από το Τμήμα Ανοσολογίας – Ιστοσυμβατότητας του Νοσοκομείου Λαϊκό μέσω ηλεκτρονικού ταχυδρομείου δύναται να αποτελέσει νόμιμο τρόπο ικανοποίησης του δικαιώματος πρόσβασης, υπό τους προαναφερθέντες ανωτέρω όρους και προϋποθέσεις.
2) Το Νοσοκομείο Λαϊκό, ως υπεύθυνος επεξεργασίας, οφείλει να τηρεί τους όρους του απορρήτου και της ασφάλειας της επεξεργασίας που περιγράφονται στην παρούσα, για την ασφαλή αποστολή ιατρικών αποτελεσμάτων στους ενδιαφερόμενους ασθενείς από το Τμήμα Ανοσολογίας – Ιστοσυμβατότητας του Νοσοκομείου.

Ο Πρόεδρος **Η Γραμματέας**

Πέτρος Χριστόφορος **Ειρήνη Παπαγεωργοπούλου**