ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 15-11-2013

Αριθ. Πρωτ.: Γ/ΕΞ/7295/15-11-2013

Α Π Ο Φ Α Σ Η ΑΡ. 138/2013

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση στην έδρα της την 06-11-2013, σε συνέχεια της από 20-06-2013 τακτικής συνεδρίασής της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Π. Χριστόφορος, Πρόεδρος της Αρχής, και τα τακτικά μέλη της Αρχής Λ. Κοτσαλής, Αν. – Ιωάν. Μεταξάς, Δ. Μπριόλας, Α. Συμβώνης, ως εισηγητής, και Π. Τσαντίλας. Το τακτικό μέλος Κ. Χριστοδούλου, αν και προσκλήθηκε νομίμως, δεν προσήλθε λόγω κωλύματος. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, οι Λ. Ρούσσος, ειδικός επιστήμων-πληροφορικός, και Κ. Λιμνιώτης, ειδικός επιστήμων-πληροφορικός, ως βοηθοί εισηγητή, ενώ απουσίαζαν λόγω κωλύματος οι βοηθοί εισηγητή Ε. Σιουγλέ, ειδική επιστήμων-πληροφορικός, και Ι. Λυκοτραφίτης, ειδικός επιστήμων-πληροφορικός. Επίσης, παρέστη, με εντολή του Προέδρου, και η Μ. Γιαννάκη, υπάλληλος του Διοικητικού – Οικονομικού Τμήματος της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Με το ν. 3892/2010 θεσπίστηκε το σύστημα Ηλεκτρονικής Συνταγογράφησης (εφεξής ΣΗΣ), το οποίο περιλαμβάνει την ηλεκτρονική καταχώρηση και εκτέλεση συνταγών και παραπεμπτικών. Σκοποί του συστήματος, όπως προβλέπονται στον ανωτέρω νόμο, είναι: α) η υποστήριξη των Φορέων Κοινωνικής Ασφάλισης (Φ.Κ.Α), τόσο για τον έλεγχο και την εκκαθάριση των συνταγών και παραπεμπτικών, όσο και για την κάλυψη των δαπανών φαρμακευτικής περίθαλψης και υπηρεσιών υγείας, β) η υποστήριξη του ελέγχου για όλες τις

υπηρεσίες υγείας που παρέχονται προς τους ασφαλισμένους των Φ.Κ.Α., γ) η υποστήριξη της παρακολούθησης και ελέγχου της συνταγογράφησης, της συγκέντρωσης και στατιστικής αξιολόγησης στοιχείων που έχουν σχέση με παροχές υγείας και φαρμακευτικής περίθαλψης, δ) η υποστήριξη της εποπτείας και του συντονισμού ενεργειών για τον έλεγχο των δαπανών του συστήματος υγειονομικής περίθαλψης όλων των φορέων και κλάδων ασθένειας αρμοδιότητας της Γενικής Γραμματείας Κοινωνικών Ασφαλίσεων. Σύμφωνα με το άρθρο 6 του ν. 3892/2010, η Γενική Γραμματεία Κοινωνικών Ασφαλίσεων (εφεξής ΓΓΚΑ) είναι υπεύθυνη για τη δημιουργία και λειτουργία της βάσης δεδομένων της ηλεκτρονικής συνταγογράφησης. Η βάση λειτουργεί με την εποπτεία της Υπηρεσίας Ελέγχου Δαπανών Υγείας Φορέων Κοινωνικής Ασφάλισης (εφεξής, ΥΠΕΔΥΦΚΑ) και της Διεύθυνσης Μηχανογραφικών Εφαρμογών που υπάγονται στη ΓΓΚΑ. Περαιτέρω, ο φορέας «Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης – ΗΔΙΚΑ Α.Ε.» (εφεξής ΗΔΙΚΑ) τηρεί και συντηρεί την ανωτέρω βάση για λογαριασμό της ΓΓΚΑ.

Βάσει των ανωτέρω και μετά από την υπ' αριθμ. πρωτ. ΓΝ/ΕΙΣ/1037/06-09-2010 γνωστοποίηση της ΓΓΚΑ προς την Αρχή, η Αρχή εξέδωσε την υπ' αριθμ. πρωτ. ΓΝ/ΕΞ/350/31-03-2011 και με αριθμό 1039 άδεια ίδρυσης και λειτουργίας αρχείου με ευαίσθητα δεδομένα προς τη ΓΓΚΑ για την επεξεργασία ευαίσθητων προσωπικών δεδομένων μέσω του ΣΗΣ. Στην ανωτέρω άδεια η Αρχή προσδιόρισε συγκεκριμένους όρους αναφορικά με τη νομιμότητα και την ασφάλεια της επεξεργασίας, τους οποίους οφείλει να ικανοποιήσει ο υπεύθυνος της επεξεργασίας (ΓΓΚΑ).

Σε συνέχεια της έκδοσης της άδειας, η Αρχή πραγματοποίησε, στο πλαίσιο του ετήσιου πλάνου των τακτικών ελέγχων της, επιτόπιο έλεγχο στο ΣΗΣ αναφορικά με την προστασία και την ασφάλεια των προσωπικών δεδομένων[1]. Καθώς η λειτουργία και διατήρηση του συστήματος ΣΗΣ έχει ανατεθεί πλήρως στην ΗΔΙΚΑ από την ΓΓΚΑ, ο έλεγχος έλαβε χώρα εξ ολοκλήρου στις εγκαταστάσεις της ΗΔΙΚΑ (εκτελών την επεξεργασία) και υπεργολάβων αυτής. Ο έλεγχος έγινε σε δύο στάδια, ειδικότερα:

α) Το πρώτο στάδιο του ελέγχου πραγματοποιήθηκε στις 22-23/11/2011 στις εγκαταστάσεις της ΗΔΙΚΑ στην οδό Λαγουμιτζή 40, στο Ν. Κόσμο, από τους ελεγκτές της Αρχής Κωνσταντίνα Καμπουράκη, Κωνσταντίνο Μουλίνο, Ευφροσύνη Σιουγλέ, Ιωάννη Λυκοτραφίτη, Λεωνίδα Ρούσσο και Κωνσταντίνο Λιμνιώτη, μετά από την υπ' αριθμ. πρωτ.

[1] Κατά το άρθρο 19 παρ. 1 στοιχ. η) του ν. 2472/1997 «Η Αρχή έχει τις εξής ιδίως αρμοδιότητες :… η) Ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους στο πλαίσιο των οποίων ελέγχονται η τεχνολογική υποδομή και άλλα, αυτοματοποιημένα ή μη, μέσα που υποστηρίζουν την επεξεργασία των δεδομένων. Έχει προς τούτο δικαίωμα προσβάσεως στα δεδομένα προσωπικού χαρακτήρα και συλλογής κάθε πληροφορίας για τους σκοπούς του ελέγχου, χωρίς να μπορεί να της αντιταχθεί κανενός είδους απόρρητο…».

Γ/ΕΞ/7588/15-11-2011 εντολή του Προέδρου της Αρχής. Ακολούθως, δεδομένου ότι στη σχετική σύμβαση της ΗΔΙΚΑ με την εταιρεία IONIS προβλεπόταν, ως υπεργολάβος εταιρεία για το ΣΗΣ η εταιρεία Computer Studio Α.Ε., οι ελεγκτές της Αρχής Κωνσταντίνα Καμπουράκη, Λεωνίδας Ρούσσος και Κωνσταντίνος Λιμνιώτης πραγματοποίησαν συμπληρωματικό επιτόπιο έλεγχο στις 28-03-2012 στις εγκαταστάσεις της Computer Studio Α.Ε. στη Λ. Βουλιαγμένης 223 στη Δάφνη, προκειμένου να αποσαφηνιστούν ειδικότερα ζητήματα, κυρίως επί της ανάπτυξης και διαχείρισης της εφαρμογής.

β) Το δεύτερο στάδιο του ελέγχου ξεκίνησε το Μάιο του 2012 όταν γνωστοποιήθηκε στην Αρχή, μέσω τηλεφωνικής επικοινωνίας με αρμόδιο υπάλληλο της ΗΔΙΚΑ, ότι η προηγούμενη έκδοση του ΣΗΣ είχε ήδη παραδοθεί από την Computer Studio Α.Ε. βάσει της σχετικής σύμβασης, καθώς επίσης και ότι η ΗΔΙΚΑ είχε αναπτύξει εξ αρχής μία νέα εφαρμογή για το ΣΗΣ, η οποία και θα αντικαθιστούσε την παλαιότερη στο αμέσως προσεχές χρονικό διάστημα. Κατόπιν τούτου, κλιμάκιο ελεγκτών της Αρχής αποτελούμενο από τους Ιωάννη Λυκοτραφίτη, Λεωνίδα Ρούσσο και Κωνσταντίνο Λιμνιώτη πραγματοποίησε εκ νέου επίσκεψη στις εγκαταστάσεις της ΗΔΙΚΑ στις 15-05-2012, στο πλαίσιο της οποίας δόθηκαν περισσότερες πληροφορίες για τη νέα υλοποίηση του ΣΗΣ (η οποία, κατά τη στιγμή του εν λόγω επιτόπιου ελέγχου, δεν είχε τεθεί ακόμη σε λειτουργία). Παράλληλα, με την επίσκεψη αυτή, ζητήθηκαν διευκρινίσεις επί του περιστατικού ασφαλείας το οποίο είχε λάβει χώρα περί τα μέσα Απριλίου 2012 και αφορούσε στο ΣΗΣ, το οποίο και είχε γίνει ευρέως γνωστό από τα Μέσα Μαζικής Ενημέρωσης. Περαιτέρω διευκρινίσεις σχετικά με το εν λόγω περιστατικό ζητήθηκαν ακολούθως από την Αρχή και με το υπ' αριθμ. πρωτ. Α/ΕΞ/84/28-05-2012 έγγραφο, στο οποίο η ΗΔΙΚΑ απάντησε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5862/13-09-2012 έγγραφο, ενώ υπέβαλε και συμπληρωματικά έγγραφα τα οποία έλαβαν αριθμ. πρωτ. Α/ΕΙΣ/165/13-11-2012. Τέλος, λαμβάνοντας υπόψη τα παραπάνω, πραγματοποιήθηκε νέος επιτόπιος έλεγχος για την αναθεωρημένη έκδοση του ΣΗΣ από τους ελεγκτές της Αρχής Ευφροσύνη Σιουγλέ, Λεωνίδα Ρούσσο και Κωνσταντίνο Λιμνιώτη στις 1-10-2012 και 11-10-2012, μετά την υπ' αριθμ. πρωτ. Γ/ΕΞ/6183/28-09-2012 εντολή ελέγχου του Προέδρου της Αρχής.

Ο έλεγχος του ΣΗΣ (και στα δύο στάδια), εστιάστηκε σε επίπεδο διαδικασιών αλλά και σε τεχνικά ζητήματα, βάσει εσωτερικού πλάνου ελέγχου που καταρτίστηκε από τους ελεγκτές-μέλη των ομάδων ελέγχου, προσαρμοσμένου στο συγκεκριμένο σύστημα. Ειδικότερα, ο έλεγχος περιλάμβανε:

α) Ειδικό έλεγχο αναφορικά με την εκπλήρωση των υποχρεώσεων του υπεύθυνου επεξεργασίας ως προς τους όρους της άδειας που έχει εκδώσει η Αρχή.

β) Γενικό έλεγχο αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων του ΣΗΣ ως προς τους παρακάτω τομείς: i) Οργάνωση – διαδικασίες ως προς την ασφάλεια: πολιτική και σχέδιο ασφάλειας, υπεύθυνος ασφάλειας, σχέδιο ανάκαμψης από καταστροφές, κώδικας δεοντολογίας του προσωπικού, εκπαίδευση του προσωπικού, εταιρείες-ανάδοχοι, διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων, διαδικασίες ελέγχου ευπαθειών, διαδικασίες καταστροφής δεδομένων, ii) Μέτρα φυσικής ασφάλειας, iii) Τεχνικά μέτρα ασφάλειας: ασφάλεια δικτύου/επικοινωνιών, ασφάλεια υπολογιστών, διαχείριση χρηστών, ασφάλεια εφαρμογής, ασφάλεια βάσης δεδομένων, διαδικασίες ανάπτυξης εφαρμογών, έλεγχος χρήσης πληροφοριακών πόρων, αρχεία καταγραφής.

Στο πλαίσιο των επιτόπιων ελέγχων ζητήθηκε από τους εκπροσώπους της ΗΔΙΚΑ η επίδοση μιας σειρά πειστηρίων (εγγράφων και ηλεκτρονικών). Για τη διασφάλιση της ακεραιότητας των ηλεκτρονικών πειστηρίων εφαρμόστηκε αλγόριθμος κατακερματισμού (MD5 hash) με χρήση κατάλληλου λογισμικού. Η λίστα των πειστηρίων, σε κάθε επιτόπιο έλεγχο, εκτυπώθηκε σε δύο (2) αντίγραφα και υπογράφηκε από τα μέλη της ομάδας ελέγχου, καθώς και από τους εκπροσώπους της ΗΔΙΚΑ.

Για τα δύο στάδια του ελέγχου (παλαιό και νέο ΣΗΣ) συντάχθηκαν, από τους ελεγκτές των ομάδων ελέγχου, τα σχετικά Πρακτικά ελέγχου, στα οποία καταγράφονται οι απαντήσεις/διευκρινήσεις της ΗΔΙΚΑ, καθώς και οι επιτόπιες παρατηρήσεις των ελεγκτών της Αρχής (αρ.πρωτ. Γ/ΕΞ/5175/27-07-2012 και Γ/ΕΞ/8119/18-12-2012) . Εν συνεχεία, τα μέλη των ομάδων ελέγχου μελέτησαν τα Πρακτικά σε συνδυασμό με το σύνολο των πειστηρίων, καθώς και τα συμπληρωματικά στοιχεία (έντυπα, κείμενα κτλ.) που είχαν αποσταλεί στην Αρχή από την ΗΔΙΚΑ ή/και την Computer Studio Α.Ε. καθ’ όλη τη διάρκεια του ελέγχου, και συνέταξαν Πόρισμα, το οποίο υποβλήθηκε στην Αρχή με το υπ’ αριθμ. πρωτ. Γ/ΕΙΣ/1792/11-03-2013 έγγραφο (εφεξής «Πόρισμα του ελέγχου»). Αναλυτική αναφορά όλων των πειστηρίων, αλλά και των λοιπών συμπληρωματικών στοιχείων, υπάρχει στο Πόρισμα του ελέγχου.

Στο εμπιστευτικό Πόρισμα του ελέγχου καταγράφονται, μεταξύ άλλων, τα ευρήματα αναφορικά με ελλιπή μέτρα ασφάλειας ή διαδικασίες προστασίας προσωπικών δεδομένων που εντοπίστηκαν, οι σχετικοί κίνδυνοι που απορρέουν, καθώς επίσης και οι προτεινόμενες από τα μέλη των ομάδων ελέγχου συστάσεις για την αντιμετώπιση των κινδύνων που δημιουργούνται. Ειδικότερα, τα ευρήματα σχετίζονται αφενός με τη μη εκπλήρωση όρων της άδειας της Αρχής και αφετέρου με τη συνολική ασφάλεια της επεξεργασίας των προσωπικών δεδομένων (άρθρο 10 του ν. 2472/1997). Η αναλυτική παρουσίαση των ευρημάτων, των σχετικών κινδύνων, καθώς και των προτεινόμενων συστάσεων των ελεγκτών καταγράφονται

στο Πόρισμα του ελέγχου.

Η ΓΓΚΑ κλήθηκε, ως υπεύθυνος επεξεργασίας, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/3887/06-06-2013 έγγραφο της Αρχής, νομίμως σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 20-06-2013 για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει διεξοδικά τις απόψεις της επί των ανωτέρω. Το ίδιο έγγραφο κοινοποιήθηκε και στην ΗΔΙΚΑ, με την επισήμανση ότι κρίνεται σκόπιμο να παρίστανται στην εν λόγω συνεδρίαση και εκπρόσωποί της. Μαζί με την κλήση, επιδόθηκε απόσπασμα από το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4574/08-07-2013 πόρισμα του ελέγχου. Στη συνεδρίαση της Αρχής, την 20-06-2013, παρέστησαν νομίμως, ο … ως εκπρόσωπος της ΓΓΚΑ, και οι …, ως εκπρόσωποι της ΗΔΙΚΑ. Κατά την ακρόαση, οι ως άνω εκπρόσωποι εξέθεσαν προφορικά τις απόψεις τους. Κατόπιν της ακρόασης, η ΗΔΙΚΑ κατέθεσε εμπροθέσμως σχετικό υπόμνημα με το υπ' αριθμ. πρωτ. 9363/04-07-2013 έγγραφο (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/4484/04-07-2013). Η ΗΔΙΚΑ, στο ως άνω υπόμνημά της, καταγράφει, για κάθε εύρημα που αναφέρεται στο πόρισμα του ελέγχου, τις απόψεις της, καθώς επίσης και τα μέτρα στα οποία προέβη για την αντιμετώπιση του κάθε σχετικού κινδύνου.

Η Αρχή, μετά από εξέταση των προαναφερομένων στοιχείων, αφού αναγνώστηκαν τα πρακτικά της συνεδρίασης της 20-06-2013, άκουσε τον εισηγητή και τους βοηθούς εισηγητή, οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Μέσω του συστήματος ΣΗΣ πραγματοποιείται επεξεργασία ευαίσθητων προσωπικών δεδομένων όπως αυτά ορίζονται στο άρθρο 2 του ν. 2472/1997. Υπεύθυνος επεξεργασίας, κατά το άρθρο 2 εδ. ζ) του ν. 2472/1997, είναι η ΓΓΚΑ, στην οποία έχει χορηγηθεί και η σχετική άδεια της Αρχής, ενώ η ΗΔΙΚΑ αποτελεί εκτελούσα την επεξεργασία, κατά την έννοια του άρθρου 2 εδ. η) του ν. 2472/1997.

2. Επισημαίνεται ότι το είδος των προσωπικών δεδομένων που υφίστανται επεξεργασία στο πλαίσιο λειτουργίας του ΣΗΣ (ήτοι αναλυτικά δεδομένα υγείας του συνόλου των ασφαλισμένων της χώρας, τα οποία καθίστανται προσβάσιμα σε εξουσιοδοτημένους χρήστες μέσω Διαδικτύου) καθιστά την επεξεργασία εξόχως κρίσιμη, αφού οποιαδήποτε τυχόν αθέμιτη επεξεργασία τους συνιστά ιδιαίτερα έντονη προσβολή του δικαιώματος στην προστασία των προσωπικών δεδομένων. Κατά συνέπεια, τόσο η ΓΓΚΑ, ως υπεύθυνος επεξεργασίας, όσο και η ΗΔΙΚΑ, ως εκτελούσα την επεξεργασία, οφείλουν, κατ' εφαρμογή των οριζομένων στο άρθρο 10 παρ. 3 και 4 του ν. 2472/1997, να εξασφαλίζουν το μέγιστο

δυνατό επίπεδο ασφάλειας. Με αυτό το σκεπτικό, εξάλλου, η Αρχή έθεσε, στην άδεια που εξέδωσε για το ΣΗΣ, και τους ελάχιστους όρους και προϋποθέσεις για την προστασία των προσωπικών δεδομένων.

3. Σύμφωνα με την με αρ. 1039 άδεια της Αρχής για το ΣΗΣ, ο υπεύθυνος επεξεργασίας οφείλει, μεταξύ άλλων, να ικανοποιήσει τους παρακάτω ειδικούς όρους ως προς την επεξεργασία των ευαίσθητων προσωπικών δεδομένων:

α) Μέσα σε ένα χρόνο από την ημερομηνία χορήγησης της άδειας να εκπονήσει μελέτη επικινδυνότητας, πολιτική ασφάλειας και σχέδιο ασφάλειας και να υποβάλει τα σχετικά κείμενα στην Αρχή. Επίσης, να υποβάλει στην Αρχή κείμενο κώδικα δεοντολογίας σχετικά με την προστασία των προσωπικών δεδομένων, ειδικά για το προσωπικό που δεν καλύπτεται από το ιατρικό απόρρητο.

β) Να λάβει τα κατάλληλα μέτρα ώστε η εγγραφή –με σκοπό τη συμμετοχή– στο σύστημα ΣΗΣ να πραγματοποιείται με ασφαλή τρόπο αναγνώρισης των χρηστών. Ενδεικτικά, αναφέρεται ως παράδειγμα στην άδεια, ότι η εγγραφή των ιατρών θα πρέπει να ενεργοποιείται μόνο μετά από επαλήθευση της ταυτότητάς τους και της ιδιότητάς τους ως ιατρών που νομίμως ασκούν το επάγγελμα και ως ιατρών συμβεβλημένων με τους Φορείς Κοινωνικής Ασφάλισης (ΦΚΑ) (π.χ. με έλεγχο των συμβάσεων με τους ΦΚΑ ή με άλλα μέσα, όπως με χρήση «έξυπνων καρτών» που πιστοποιούν και την ιδιότητά τους ως μέλη των ιατρικών συλλόγων).

γ) Να λάβει τα κατάλληλα μέτρα, ώστε η πρόσβαση στο σύστημα ΣΗΣ να περιορίζεται στα αναγκαία στοιχεία για τον συγκεκριμένο κάθε φορά επιδιωκόμενο σκοπό. Ειδικότερα, ο Γενικός Γραμματέας Κοινωνικών Ασφαλίσεων και η ΥΠΕΔΥΦΚΑ να έχουν πρόσβαση μόνο στα στοιχεία που είναι κάθε φορά αναγκαία για την εκτέλεση των κατά νόμων αρμοδιοτήτων τους. Οι ΦΚΑ, οι φαρμακοποιοί, οι μονάδες παροχής υπηρεσιών υγείας και οι ιατροί να έχουν πρόσβαση μόνο στα στοιχεία της βάσης που αφορούν τον εκάστοτε ΦΚΑ ή οι ίδιοι παράγουν. Κατ΄ εξαίρεση, ο ιατρός δύναται να έχει πρόσβαση για τον προσδιορισμό της κατάλληλης φαρμακευτικής αγωγής (π.χ. προκειμένου να μη συνταγογραφεί φάρμακα που έχουν αποδειχθεί αναποτελεσματικά για τον συγκεκριμένο ασθενή) στα δεδομένα τυχόν προηγούμενης φαρμακευτικής αγωγής ή ιατρικών πράξεων που έχουν καταχωριστεί από άλλους ιατρούς, με την προϋπόθεση ότι ο ασθενής έχει ενημερωθεί σχετικά και συναινεί στην πρόσβαση αυτή (άρθρο 3 παρ. 8 του ν. 3892/2010). Για το σκοπό αυτό ο υπεύθυνος επεξεργασίας πρέπει το αργότερο μέχρι την επόμενη ανανέωση της άδειας (η ισχύς της άδειας είναι μέχρι 28/02/2014), να εφαρμόσει τα κατάλληλα μέτρα ασφάλειας που διασφαλίζουν ότι η πρόσβαση του ιατρού, χρήστη του ΣΗΣ, στα δεδομένα ασθενών σχετικά

με προηγούμενη φαρμακευτική αγωγή ή ιατρικές πράξεις που έχουν καταχωριστεί από άλλους ιατρούς πραγματοποιείται, όπως ορίζει το άρθρο 3 παρ. 8 του ν. 3892/2010, με τη ρητή και ειδική συγκατάθεση του ασθενούς (π.χ. μέσω ηλεκτρονικής κάρτας υγείας, την οποία φέρει ο ίδιος ο ασθενής). Σε κάθε περίπτωση το γεγονός και οι λεπτομέρειες της πρόσβασης θα πρέπει να μπορούν να ελεγχθούν εκ των υστέρων (μέσω της λειτουργίας κατάλληλων αρχείων καταγραφής - log files).

δ) Τα δεδομένα προσωπικού χαρακτήρα, σύμφωνα με τα οριζόμενα στο άρθρο 4 παρ. 1 στοιχ. δ΄ του ν. 2472/1997, πρέπει να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται για την πραγματοποίηση των σκοπών της επεξεργασίας τους, και πάντως όχι πλέον της 20ετίας από την τελευταία επίσκεψη του ασθενή.

ε) Αποδέκτες των δεδομένων είναι οι ιατροί, οι φαρμακοποιοί, οι μονάδες παροχής υπηρεσιών υγείας και οι ΦΚΑ, στο μέτρο που έχουν πρόσβαση στο σύστημα, οι αρμόδιες εισαγγελικές και δικαστικές αρχές, καθώς και άλλα πρόσωπα ή δημόσιες αρχές εφόσον η διαβίβαση δεδομένων προβλέπεται από διάταξη νόμου ή δικαστική απόφαση.

4. Αναφορικά με την ασφάλεια της επεξεργασίας, το άρθρο 10 παρ. 3 του ν. 2472/1997 ορίζει ότι: «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».

Επισημαίνεται ότι οι υποχρεώσεις του νόμου βαρύνουν τον υπεύθυνο επεξεργασίας, προς τον οποίον, κατά συνέπεια, απευθύνονται συστάσεις κατά το άρθρο 19 παρ. 1 γ) του ν. 2472/1997 και επιβάλλονται οι κυρώσεις του άρθρου 21 του ιδίου νόμου. Ο γενικός αυτός κανόνας ακολουθείται και ως προς την υποχρέωση του υπευθύνου επεξεργασίας να λαμβάνει κατά το άρθρο 10 παρ. 3 τα κατάλληλα μέτρα ασφάλειας. Η ύπαρξη εκτελούντος την επεξεργασία κατά την παρ. 4 του ιδίου άρθρου δεν απαλλάσσει τον υπεύθυνο από τη δική του υποχρέωση – αντιθέτως, η υποχρέωση βαρύνει αναλόγως και τον εκτελούντα, έτσι ώστε η ανάθεση της επεξεργασίας να μην αποδυναμώνει την προστασία των δεδομένων.

5. Σύμφωνα με το Πόρισμα του ελέγχου της Αρχής, διαπιστώθηκαν ελλείψεις του υπεύθυνου επεξεργασίας ως προς την εκπλήρωση των υπό το στοιχείο 2 α), β), και γ) αναφερόμενων όρων της άδειας. Κάποιες ελλείψεις και παραλείψεις διαπιστώθηκαν επίσης και αναφορικά με τα οργανωτικά και τεχνικά μέτρα ασφάλειας που έχουν ληφθεί για το

ΣΗΣ, οι οποίες αφορούν –μεταξύ άλλων– στη μη επαρκή τεκμηρίωση των εφαρμοζόμενων μέτρων ασφαλείας, καθώς και στη μη συστηματική επίβλεψή τους.

6. Με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4484/04-07-2013 υπόμνημα, η ΗΔΙΚΑ ενημέρωσε την Αρχή ότι ελήφθησαν μέτρα[2] για την αντιμετώπιση των κινδύνων που επισημαίνονται στο Πόρισμα του ελέγχου, καθώς επίσης και για τη συμμόρφωση με τους όρους της άδειας. Περαιτέρω, στο υπόμνημα αναφέρεται ότι για το ολοκληρωμένο ΣΗΣ έχει ενταχθεί Οριζόντια Πράξη στο ΕΣΠΑ με τίτλο «Ανάπτυξη συστήματος Ηλεκτρονικής Συνταγογράφησης και παροχή σχετικών Υποστηρικτικών Υπηρεσιών», ενώ ο σχετικός διαγωνισμός βρίσκεται στο στάδιο της ολοκλήρωσης της τεχνικής αξιολόγησης των προσφορών. Για διάφορα ανοιχτά ζητήματα, τα οποία θίγονται και στο πόρισμα του ελέγχου, υπάρχει σχετική πρόβλεψη στις προδιαγραφές που τίθενται στο διαγωνισμό.

7. Μετά την εξέταση όλων των ανωτέρω στοιχείων, προκύπτουν τα εξής αναφορικά με την εκπλήρωση των όρων της άδειας της Αρχής:

α) Μέσω του ΣΗΣ, είναι εφικτό σε κάποιον ιατρό να αναζητήσει ιατρικό ιστορικό ασθενούς χωρίς να έχει τη συγκατάθεσή του (στην τρέχουσα υλοποίηση του συστήματος, ο ιατρός απλά επιλέγει, σε κατάλληλο «παράθυρο» της εφαρμογής και πριν δει το ιστορικό του ασθενούς, ότι έχει τη συγκατάθεσή του, ενώ η δήλωση αυτή του ιατρού καταγράφεται).

Η προσπέλαση ιατρικού ιστορικού ασθενούς από ιατρό μέσω του ΣΗΣ, χωρίς τη λήψη συγκατάθεσης, αποτελεί παράβαση του υπό του στοιχείου 3 γ) αναφερόμενου όρου της άδειας της Αρχής. Η Αρχή αναγνωρίζει το ότι η μη δυνατότητα χρήσης ασφαλών ψηφιακών πιστοποιητικών για τους ασφαλισμένους δυσχεραίνει την υλοποίηση μηχανισμού λήψης ρητής και ειδικής συγκατάθεσης στο περιβάλλον του ΣΗΣ. Ωστόσο, ο υπεύθυνος επεξεργασίας οφείλει σε κάθε περίπτωση να λάβει τα απαραίτητα μέτρα ώστε να διασφαλίζεται ότι δεν πραγματοποιούνται προσβάσεις χωρίς τη ρητή και ειδική συναίνεση του ασθενούς. Ως εκ τούτου, ο υπεύθυνος επεξεργασίας, σε συνεργασία με τον εκτελούντα την επεξεργασία, ο οποίος τηρεί και συντηρεί το ΣΗΣ, θα πρέπει να εξετάσει την πλέον πρόσφορη λύση για την αντιμετώπιση του εν λόγω ζητήματος, η οποία θα συμπληρώνει την υπάρχουσα υλοποίηση. Προς αυτήν την κατεύθυνση, κρίνεται απαραίτητο να εξεταστεί η λήψη των κάτωθι μέτρων:

i) Καθορισμός διαδικασίας συστηματικού και τακτικού ελέγχου των προσβάσεων των χρηστών του ΣΗΣ σε ιατρικά ιστορικά ασθενών, έτσι ώστε να μπορούν να ανιχνευθούν

[2] Κάποια εξ αυτών είχαν ήδη ληφθεί πριν την ολοκλήρωση της σύνταξης του πορίσματος του ελέγχου.

τυχόν παράνομες προσβάσεις.

ii) Ενημέρωση των ασφαλισμένων για το ποιοι χρήστες του ΣΗΣ απέκτησαν πρόσβαση στα προσωπικά τους δεδομένα, μέσω π.χ. αυτοματοποιημένων και αποδοτικών διαδικασιών ικανοποίησης του δικαιώματος πρόσβασης κατά το άρθρο 12 του ν. 2472/1997 ή/και αυτόματης αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου (email)/σύντομου γραπτού μηνύματος (sms) στον ασφαλισμένο κάθε φορά που πραγματοποιείται πρόσβαση στο ιατρικό του ιστορικό, τουλάχιστον για τις περιπτώσεις που η πρόσβαση αυτή δεν συνοδεύεται από την ηλεκτρονική καταχώρηση συνταγής.

β) Για την αρχική ταυτοποίηση των χρηστών (ιατροί/φαρμακοποιοί), κατά την εγγραφή τους στο σύστημα δεν απαιτείται η φυσική τους παρουσία, ούτε γίνεται χρήση ψηφιακών πιστοποιητικών αυτών. Η ταυτοποίηση βασίζεται στο ότι ζητείται από τον εκάστοτε υποψήφιο χρήστη να υποβάλει ηλεκτρονικά πλήθος προσωπικών του στοιχείων (αρ. άδειας ασκήσεως επαγγέλματος, έτος λήψης ειδικότητας, Α.Μ. ΤΣΑΥ κ.ά.), τα οποία ακολούθως ελέγχονται στο μητρώο του ΤΣΑΥ.

Στο ως άνω υπόμνημα αναφέρεται ότι στο σχετικό διαγωνισμό που είναι σε εξέλιξη προβλέπονται ισχυροί μηχανισμοί ταυτοποίησης και αυθεντικοποίησης των χρηστών (τόσο για τους επαγγελματίες υγείας όσο και για τους διαχειριστές), μέσω «έξυπνων καρτών» ή ισοδύναμου μηχανισμού.

Σε κάθε περίπτωση, επισημαίνεται ότι οι κανόνες και πρότυπα αναφορικά με την εγγραφή, ταυτοποίηση και ηλεκτρονική αναγνώριση πολιτών σε ηλεκτρονικές υπηρεσίες του δημόσιου τομέα καθορίζονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (ΥΑΠ Φ.40.4/1/989, ΦΕΚ 1301/Β/2012) και, ειδικότερα, στο Παράρτημα ΙΙΙ αυτού (Πλαίσιο Ψηφιακής Αυθεντικοποίησης). Όπως επισημαίνεται στο εν λόγω Πλαίσιο, οι διαδικασίες εγγραφής (και αυθεντικοποίησης) των χρηστών καθορίζονται από το επίπεδο εμπιστοσύνης στο οποίο εντάσσονται οι παρεχόμενες ηλεκτρονικές υπηρεσίες. Για το ΣΗΣ, όπου γίνεται επεξεργασία ευαίσθητων προσωπικών δεδομένων, οι διαδικασίες εγγραφής των χρηστών θα πρέπει να αντιστοιχούν στο υψηλότερο επίπεδο εγγραφής (ήτοι 3, όπως αυτό ορίζεται επίσης στο Πλαίσιο).

γ) Δεν υπάρχει κώδικας δεοντολογίας για το προσωπικό που επεξεργάζεται δεδομένα του ΣΗΣ και δεν δεσμεύεται από απόρρητο (π.χ. ιατρικό), ο οποίος να έχει εγκριθεί από τον υπεύθυνο επεξεργασίας και να εφαρμόζεται από τον εκτελούντα[3]. Σημειώνεται ότι

[3] Ο κώδικας δεοντολογίας που επισυνάπτεται στο υπόμνημα της ΗΔΙΚΑ δεν θεωρείται επαρκής, αφού δεν αποτυπώνει τους κανόνες που πρέπει να ακολουθούν οι υπάλληλοι στο πλαίσιο της διαφύλαξης της ασφάλειας των δεδομένων του ΣΗΣ

στο αντίγραφο της σύμβασης προσωπικού γίνεται αναφορά στις διατάξεις του Κανονισμού «Οργανισμού του ΚΗΥΚΥ» που ισχύει μεταβατικά και για την ΗΔΙΚΑ, και όπου υποχρεώσεις και δικαιώματα των υπαλλήλων προβλέπονται στο Κεφάλαιο ΣΤ' του ανωτέρω Κανονισμού. Δεν υπάρχει ωστόσο εγκεκριμένος κώδικας δεοντολογίας ειδικά για το ΣΗΣ. Η ανωτέρω έλλειψη –πέραν του ότι αποτελεί όρο της άδειας– ενδεχομένως οδηγήσει σε μη εξουσιοδοτημένες ενέργειες αναφορικά με την επεξεργασία προσωπικών δεδομένων στο ΣΗΣ, με επίκληση άγνοιας της δέουσας συμπεριφοράς.

Κατά συνέπεια, θα πρέπει να καταρτιστεί –ειδικά για το ΣΗΣ– κώδικας δεοντολογίας για το προσωπικό αναφορικά με την προστασία των προσωπικών δεδομένων, ο οποίος θα πρέπει να είναι εγκεκριμένος από τον υπεύθυνο επεξεργασίας. Όλοι οι υπάλληλοι του εκτελούντος την επεξεργασία, αλλά και εξωτερικοί συνεργάτες, θα πρέπει να δεσμεύονται εγγράφως για την τήρηση της εχεμύθειας και εμπιστευτικότητας, τόσο κατά τη διάρκεια της απασχόλησής τους όσο και μετά την αποχώρησή τους.

Συνεπώς, στη λειτουργία του ΣΗΣ, υπάρχουν ακόμα ελλείψεις αναφορικά με τους υπό το στοιχείο 3 α), β) και γ) αναφερόμενους όρους της άδειας.

8. Περαιτέρω, διάφορα ζητήματα που άπτονται της ασφάλειας της επεξεργασίας κατά το άρθρο 10 του ν. 2472/1997, και τα οποία περιγράφονται στο πόρισμα του ελέγχου, χρήζουν επίσης βελτίωσης ή/και αποσαφήνισης, παρά τις σχετικές διευκρινιστικές απαντήσεις και διορθωτικές ενέργειες που περιγράφονται στο ως άνω υπόμνημα της ΗΔΙΚΑ. Τα εν λόγω ζητήματα παρατίθενται στο εμπιστευτικό παράρτημα της παρούσας.

9. Κατά συνέπεια, παρά το γεγονός ότι έχει ληφθεί –όπως προέκυψε τόσο από τον επιτόπιο έλεγχο όσο και από το ανωτέρω υπόμνημα– πλήθος τεχνικών και οργανωτικών μέτρων για την ασφάλεια της επεξεργασίας, εν τούτοις είναι ανάγκη να αντιμετωπιστούν πλήρως και τα ειδικότερα ζητήματα που τίθενται ανωτέρω. Και τούτο διότι η φύση και ο όγκος των προσωπικών δεδομένων που υφίστανται επεξεργασία μέσω του ΣΗΣ, καθώς επίσης και οι ενδεχόμενες επιπτώσεις στα υποκείμενα των δεδομένων σε περίπτωση περιστατικού παραβίασης δεδομένων, καθιστούν επιτακτική την ανάγκη λήψης των πλέον αυστηρών και αποτελεσματικών μέτρων ασφάλειας.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή καλεί τον υπεύθυνο επεξεργασίας:

1. Να υποβάλει, εντός διμήνου από την ημερομηνία έκδοσης της απόφασης, αναλυτικό χρονοδιάγραμμα για την υλοποίηση όλων των συστάσεων που αναφέρονται στο

σημείο 7 του σκεπτικού της παρούσας, καθώς επίσης και για την αντιμετώπιση των ειδικότερων ζητημάτων που τίθενται στο εμπιστευτικό παράρτημα της παρούσας. Το χρονοδιάγραμμα θα πρέπει επίσης να αφορά και σε όλα τα διορθωτικά μέτρα που προβλέπονται στον εν εξελίξει διαγωνισμό για το νέο ΣΗΣ και τα οποία δεν έχουν ακόμα υλοποιηθεί.

2. Να υποβάλλει ανά τρίμηνο περιοδικές εκθέσεις παρακολούθησης της πορείας υλοποίησης του ανωτέρω χρονοδιαγράμματος.
3. Με την αίτηση που θα υποβάλει για ανανέωση της άδειας λειτουργίας αρχείου με ευαίσθητα δεδομένα για το ΣΗΣ, να περιγράψει και τα νέα μέτρα που θα έχουν εν τω μεταξύ ληφθεί.

Ο Πρόεδρος	**Η γραμματέας**
Πέτρος Χριστόφορος	**Μελπομένη Γιαννάκη**