ΤΟΠΟΘΕΤΗΣΗ 1^{Η}: Η ανωνυμοποίηση του ΑΜΚΑ, πρέπει να γίνεται ήδη στην πηγή, δηλαδή πριν ο ΑΜΚΑ αποσταλεί στον κόμβο του e GOV Now, με ενέργειες που εκτελεί, ο εκτελών την επεξεργασία των δεδομένων, δηλαδή η εταιρεία που παρέχει και συντηρεί το Πληροφοριακό Σύστημα του κάθε Νοσοκομείου, εξασφαλίζοντας ότι καταλήγει κάθε φόρα στον ίδιο μοναδικό κωδικό, προκειμένου να τηρείται ο νόμος.

- Το άρθρο 79 του Ν.4368/2016, με τίτλο, Ηλεκτρονικό Αρχείο Υπηρεσιών Υγείας, προσέθεσε το άρθρο 13^{Α} στον Ν. 3370/2005 (Α` 176), σύμφωνα με το οποίο: *«Ως στοιχείο ταυτοποίησης του ατόμου τηρείται μοναδικός κωδικός, ο οποίος προκύπτει με κατάλληλη επεξεργασία (κωδικοποίηση) του ΑΜΚΑ και* ***αποσκοπεί στην πλήρη παρεμπόδιση της εξακρίβωσης της ταυτότητας των υποκειμένων****»*
- Στην ίδια, δε, την αιτιολογική έκθεση του Σχεδίου Νόμου, το οποίο ετέθη υπόψη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, επί τους οποίου εξεδόθη η Απόφαση 3/2015 με αριθμό πρωτοκόλλου Γ/ΕΞ/1001-1/14.07.2015 της Αρχής αναφέρεται ότι: *«Για λόγους διασφάλισης της ανωνυμίας του ασθενούς σε κεντρικό επίπεδο, τα στοιχεία ταυτοποίησης* ***πρέπει να μην είναι αναγνώσιμα από το Υπουργείο Υγείας*** *το οποίο θα συλλέγει ορισμένες αναλυτικές πληροφορίες. Για το λόγο αυτό, επιβάλλεται η κωδικοποίηση των στοιχείων ταυτοποίησής τους (ΑΜΚΑ)* ***με χρήση κρυπτογραφικών συναρτήσεων κατακερματισμού (cryptographic hash function) στην πηγή (κατά τόπους Μονάδες Υγείας),*** *οι οποίες εγγυώνται ότι η έξοδος της εφαρμογής της συνάρτησης για κάθε διαφορετική είσοδο είναι μοναδική και συνεπώς επιτρέπουν την καταγραφή και παρακολούθηση των κινήσεων επαναεισαγωγής ενός ασθενούς σε διαφορετικό χρόνο ή/και τόπο».*
- Επίσης στο Σχέδιο Νόμου, το οποίο ετέθη υπόψη της Αρχής οριζόταν ρητώς ότι: «*Τα στοιχεία ταυτοποίησης του ατόμου στηρίζονται στον ΑΜΚΑ και κωδικοποιούνται με τη χρήση κρυπτογραφικών συναρτήσεων κατακερματισμού από τον υπεύθυνο επεξεργασίας των κατά τόπο πληροφοριακών συστημάτων των Μονάδων Υγείας πριν αποσταλούν στο Υπουργείο Υγείας.*»
- Επισημαίνουμε τέλος πως η επιταγή ανωνυμοποίησης και κρυπτογράφησης του ΑΜΚΑ προκύπτει και από το κείμενου του Γενικού Κανονισμού για την Προστασία Δεδομένων (2016/679). Ενδεικτικά στην αιτιολογική σκέψη 83 αυτού αναφέρεται ότι «*για τη διατήρηση της ασφάλειας και την αποφυγή της επεξεργασίας κατά παράβαση του παρόντος κανονισμού, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα πρέπει να αξιολογεί τους κινδύνους που ενέχει η επεξεργασία και να εφαρμόζει μέτρα για τον μετριασμό των εν λόγω κινδύνων, όπως για παράδειγμα μέσω κρυπτογράφησης. Τα εν λόγω μέτρα θα πρέπει να διασφαλίζουν κατάλληλο επίπεδο ασφάλειας, πράγμα που περιλαμβάνει και την εμπιστευτικότητα (...). Κατά την εκτίμηση του κινδύνου για την ασφάλεια των δεδομένων θα πρέπει να δίνεται προσοχή στους κινδύνους που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα,*

όπως η τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία (...). Στο ίδιο πλαίσιο και το άρθρο 32 παρ. 1 περίπτωση α' του Κανονισμού προβλέπει ότι *«(...) ο εκτελών την επεξεργασία εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση: α)* ***της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα*** *(...)*»

Είναι κατά τη γνώμη μας εύληπτη η υποχρέωση των εκτελούντων την επεξεργασία να λάβουν τα ελάχιστα τεχνικά και οργανωτικά μέτρα ασφαλείας για τη μεταφορά των δεδομένων των ασθενών στον διακομιστικό κόμβο.

ΤΟΠΟΘΕΤΗΣΗ 2^{Η}: Ως «πηγή», στην οποία πρέπει να λαμβάνει χώρα ήδη- πριν τη μεταφορά – η ανωνυμοποίηση και κρυπτογράφηση των δεδομένων, νοείται το μέρος όπου είναι αποθηκευμένα και τηρούνται τα δεδομένα των ασθενών ΠΡΙΝ την διαβίβαση τους στον Διακομιστικό Κόμβο, δηλαδή αποκλειστικά η βάση δεδομένων του Νοσοκομείου, το πληροφοριακό σύστημα αυτού, στο οποίο τηρούνται κατ' αρχήν τα δεδομένα. Συνεπώς καμία άλλη βάση δεδομένων στην οποία τα δεδομένα αυτά μεταφέρονται στο πλαίσιο εκτέλεσης του Έργου (λ.χ. διακομιστικός κόμβος e GOV Now) δεν αποτελεί εναλλακτικό τόπο ή χρόνο στον οποίο δύνανται να ανωνυμοποιηθούν και να κρυπτογραφηθούν τα ήδη συλλεγέντα δεδομένα. Στο ίδιο συμπέρασμα καταλήγουμε ακόμα και εάν η έτερη βάση δεδομένων γεωγραφικά τοποθετείται εντός του Νοσοκομείου, δηλαδή στην Έδρα του Παρόχου Υγείας, με δεδομένο ότι ο Διακομιστικός Κόμβος δεν ανήκει στην κυριότητα του Παρόχου Υγείας, δηλαδή του Νοσοκομείου, αλλά στο Υπουργείο Υγείας.

Το Υπουργείο Υγείας ζητά την μεταφορά των δεδομένων των ασθενών από τα πληροφοριακά συστήματα των Νοσοκομείων, χωρίς ανωνυμοποιήση και κρυπτογράφηση τους, στη βάση δεδομένων του Διακομιστικού Κόμβου, με το αιτιολογικό ότι αυτός βρίσκεται γεωγραφικά εντός του Νοσοκομείου. Ωστόσο η θέση αυτή παραγνωρίζει το γεγονός ότι ο διακομιστικός κόμβος δεν ανήκει στην ευθύνη του Νοσοκομείου και δεν «ελέγχεται» από αυτό, αλλά από το Υπουργείο Υγείας. Συνεπώς ο διακομιστικός κόμβος – στον οποίο απαιτείται να στέλνονται μη ανωνυμοποιημένα και μη κρυπτογραφημένα δεδομένα - όχι μόνο εκφεύγει της σφαίρας εποπτείας του υπεύθυνου επεξεργασίας (το Νοσοκομείο άλλωστε παραμένει υπεύθυνος επεξεργασίας τουλάχιστον μέχρι τα δεδομένα να φτάσουν στον διακομιστικό κόμβο), αλλά επιπλέον το Υπουργείο Υγείας έχει άμεση πρόσβαση. Εν ολίγοις το Υπουργείο Υγείας απαιτώντας την αποστολή μη ανωνυμοποιημένων και μη κρυπτογραφημένων δεδομένων απευθείας στον Διακομιστικό Κόμβο του E GOV Now αποκτά δυνητικά πρόσβαση στα δεδομένα είτε απευθείας, είτε μέσω των υπεργολάβων του, οι οποίοι έχουν αναλάβει την ανωνυμοποίηση και κρυπτογράφηση των δεδομένων.

Είναι κατά τη γνώμη μας σαφές ότι το προτεινόμενο από το Υπουργείο Υγείας σχήμα αποστολής των δεδομένων στον Διακομιστικό Κόμβο θέτει υπό αμφισβήτηση την τήρηση των προϋποθέσεων του ισχύοντος νομοθετικού πλαισίου και διακινδυνεύει την επιβολή κυρώσεων στις εταιρείες μέλη του ΕΣΠΥ, τα οποία ως εκτελούντες την επεξεργασία καλούνται από το Υπουργείο Υγείας να υπερβούν τη ρητή εκ του νόμου προϋπόθεση για αποστολή ανωνυμοποιημένων και κρυπτογραφημένων δεδομένων.

ΤΟΠΟΘΕΤΗΣΗ 3^{Η}: Η ανωνυμοποίηση του ΑΜΚΑ, πρέπει να γίνει ΜΟΝΟ από τις εταιρείες που έχουν αναλάβει τη συντήρηση και υποστήριξη των πληροφοριακών συστημάτων του Νοσοκομείου ώστε να διασφαλίζεται η μη ταυτοποίηση των δεδομένων. Αυτό το σχήμα μπορεί μάλιστα να υλοποιηθεί με τρόπο που να εξασφαλίζει την ενιαία κωδικοποίηση των δεδομένων και άρα να μην αντιστρατεύεται την πραγμάτωση του σκοπού του έργου.

Είναι θεωρούμε σαφές ότι οποιοδήποτε μοντέλο μεταφοράς των δεδομένων, το οποίο μεταθέτει τον ρόλο ανωνυμοποίησης και κρυπτογράφησης των δεδομένων σε τρίτο μέρος εκτός του Νοσοκομείου και εκτός του εκτελούντα την επεξεργασία, καταλήγει αυτόματα σε δημιουργία ενός νομοθετικά ασύμβατου σχήματος.

Η τρίτη εταιρεία ανάδοχος Ανωνυμοποίησης και μεταφοράς των δεδομένων, ανωνυμοποιεί τα δεδομένα, προκειμένου να τα παραδώσει από τον Διακομιστικό στον Κεντρικό Κόμβο του Υπουργείου ανωνυμοποιημένα με σκοπό να μην δύναται να καταλήξει το Υπουργειο στην πραγματική ταυτότητα των ατόμων στα οποία αυτά ανήκουν. Ωστόσο ως ανάδοχος δημοσίου έργου, η εν λόγω εταιρεία θα πρέπει με την ολοκλήρωση του έργου να παραδώσει στην αναθέτουσα αρχή, δηλαδή στο Υπουργείο Υγείας: τον έλεγχο των διακομιστικών κόμβων και τον αλγόριθμό ανωνυμοποίησης των δεδομένων. Τίθεται επομένως θέμα ασυμβίβαστου στους δύο ρόλους καθως το Υπουργειο Υγείας: αφενός δίνει εντολή για δημιουργία κόμβων μεταφοράς δεδομένων, άρα είναι αναθέτουσα αρχή και επομένως διαθέτει πρόσβαση στα ονομαστικά δεδομένα αλλά ταυτόχρονα είναι και κάτοχος του μηχανισμού ανωνυμοποίησης και μεταφοράς δεδομένων ενώ θα έπρεπε μόνο να συγκεντρώνει τα ανώνυμα δεδομενα προς στατιστική επεξεργασία.

Όπως είναι εμφανές μάλλον αμφισβητείται η τήρηση του νόμου δεδομένου ότι το Υπουργείο: α) έχει πρόσβαση στα ονομαστικά δεδομένα και β) διαθέτει το μηχανισμό ανωνυμοποίησης αυτών και δυνητικά μπορεί να τον αναστρέψει.