ΑΝΑΣΚΟΠΗΣΗ
ΝΟΣΗΛΕΥΤΙΚΗ 2008, 47(2):202–208

Νομοθετική προστασία των ευαίσθητων προσωπικών δεδομένων στον ηλεκτρονικό φάκελο υγείας

Μαρία Μαλλιαρού
Λ/γος (ΥΝ) Νοσηλεύτρια Ψυχικής Υγείας, MSc, 492 ΓΣΝ Αλεξανδρούπολης, Αλεξανδρούπολη

Ιωσήφ Λιάσκος
Νοσηλευτής ΠΕ, MSc, Διδάκτορας Τμήματος Νοσηλευτικής, Πανεπιστήμιο Αθηνών, Αθήνα

Εργαστήριο Πληροφορικής Υγείας, Τμήμα Νοσηλευτικής, Πανεπιστήμιο Αθηνών

ΠΕΡΙΛΗΨΗ **Ο ηλεκτρονικός φάκελος υγείας είναι μια εξελισσόμενη ιδέα προσδιοριζόμενη ως μια μακροπρόθεσμη ηλεκτρονική διατήρηση πληροφοριών σχετικών με την κατάσταση της υγείας και τη φροντίδα υγείας ενός ατόμου, για όλη τη διάρκεια της ζωής του. Η συμβολή του ηλεκτρονικού φακέλου υγείας στην παροχή ποιοτικής φροντίδας υγείας, στη μείωση του κόστους των υπηρεσιών υγείας, στην αύξηση της αποδοτικότητας των επαγγελματιών υγείας αλλά και των υπολοίπων χρηστών του συντελεί στην αναγνώριση της αξίας του και στην πλήρη εφαρμογή και χρήση του στο περιβάλλον υγείας. Η αυτοματοποίηση όλων των διαδικασιών που συμβάλλουν στην παροχή υπηρεσιών υγείας, στη λήψη κρίσιμων για τη ζωή του ασθενούς αποφάσεων, στην εκπαίδευση και στην έρευνα, καθιστά επιτακτική την ανάγκη ασφάλειας των συστημάτων ηλεκτρονικών φακέλων προκειμένου να εξασφαλίζεται η εγκυρότητα, η αξιοπιστία, η διαθεσιμότητα των πληροφοριών φροντίδας υγείας αλλά και το δικαίωμα του ασθενούς στην τήρηση του απορρήτου των προσωπικών ευαίσθητων δεδομένων. Είναι ξεκάθαρο ότι το δικαίωμα του ασθενούς για διασφάλι-**

REVIEW
NOSILEFTIKI 2007, 48(2):202–208

Legislative protection of sensitive personal data in the electronic health record

Maria Malliarou
Lieutenant Psychiatric RN, MSc, 492 General Military Hospital of Alexandroupoli, Alexandroupoli, Greece

Joseph Liaskos
RN, MSc, PhD, Faculty of Nursing, University of Athens, Athens, Greece

Laboratory of Health Informatics, Faculty of Nursing, University of Athens

ABSTRACT **The electronic health record is an evolving idea determined as a long-term electronic maintenance of information about an individual's lifetime health status and health care. The contribution of the electronic patient record in quality of health care, in reduction of health services' costs, in increased efficiency of health care professionals and other users of the electronic health record, justifies its value and importance in the health care environment. The automation of all processes that contribute to the benefit of health care services, to critical decision making regarding patient's health and life, to education and research, makes electronic records' security an essential issue that ensures the validity, reliability, and availability of medical information but also the patient's right for privacy in his personal sensitive health data. It is evident that the patient's right to confidentiality in his personal data cannot be underestimated in the implementation of the electronic health record. The determination of ethic and legal guidelines and criteria relevant to the electronic acquisition, processing, and communication of personal sensitive health data, is vital.**

ση της εμπιστευτικότητας των προσωπικών του δεδομένων δεν μπορεί να υποβιβασθεί εξαιτίας της χρήσης του ηλεκτρονικού φακέλου υγείας. Ο καθορισμός ηθικών και νομικών διαδικασιών και κριτηρίων όσο αφορά στην ηλεκτρονική συλλογή, επεξεργασία και διακίνηση των ευαίσθητων προσωπικών δεδομένων ασθενών σε πιθανούς χρήστες δεδομένων υγείας είναι απαραίτητος, αφού τυχόν αποκάλυψή τους θέτει σε κίνδυνο τη σχέση τόσο ιατρού ή νοσηλευτή – ασθενή, όσο και των μελών ολόκληρης της κοινωνίας αφού είναι πιθανό από τον φόβο αποκάλυψης τους, ο ασθενής να μην εμπιστευθεί κρίσιμες πληροφορίες που αφορούν όχι μόνο στην υγεία του αλλά και στη διατήρηση της δημόσιας υγείας.

Λέξεις-κλειδιά:
• Ευαίσθητα προσωπικά δεδομένα
• Ηλεκτρονικός φάκελος υγείας

Υπεύθυνος αλληλογραφίας
Μαρία Μαλλιαρού
Νικηταρά 49, 68 100 Άγιος Βασίλειος, Αλεξανδρούπολη
Τηλ. 25510 387 32, 6944 79 64 99

A potential disclosure of patient's personal data puts at risk the relationship between patient and physician or nurse but also the one among the members of the entire society. Patients may be afraid or reluctant in revealing critical information concerning not only their personal health but also the public health.

Key words:
• Sensitive personal data
• Electronic patient record

Corresponding author
Maria Malliarou
49 Nikitara street GR-68 100 Agios Vasileios, Alexandroupoli, Greece
Tel. +30 25510 387 32, 6944 79 64 99

ΕΙΣΑΓΩΓΗ

Η επανάσταση στον χώρο των νέων τεχνολογιών επιφέρει σημαντικές αλλαγές στον τρόπο με τον οποίο αντιλαμβανόμαστε την έννοια και το περιεχόμενο της παροχής φροντίδας υγείας. Η ιατρική πληροφορία είναι από τους πιο ευαίσθητους τύπους πληροφορίας και η κακή της χρήση επηρεάζει τη ζωή του ατόμου. Παλαιότερα αυτή η πληροφορία αποθηκευόταν στα γραφεία των ιατρών χωρίς κανένας να γνωρίζει την ύπαρξη της. Προστατευόταν από το γεγονός ότι ήταν απομονωμένη, ήταν δύσκολη η πρόσβαση σ' αυτήν και ελάχιστοι γνώριζαν αν και τι συλλέγονταν και διατηρούνταν. Η πρόσβαση πλέον σε αυτή τη γνώση γίνεται μέσω των υπολογιστών ενώ λόγω των τεχνολογικών εξελίξεων και αυτή η παρεχόμενη πληροφορία έχει αυξηθεί. Για παράδειγμα υπάρχουν πλέον γενετικές πληροφορίες που παλαιότερα δεν ήταν διαθέσιμες. Η ενδεχόμενη διαρροή τέτοιων πληροφοριών σε τρίτους εγκυμονεί κινδύνους που μπορεί να επηρεάσουν ακόμη και την επαγγελματική ζωή του ατόμου (π.χ. αν θα προσληφθεί, πως θα εξελιχθεί η καριέρα του, ποιος θα είναι ο μισθός του, οι πιθανές προαγωγές του, η παραμονή του στην εργασία, κ.λπ.). Για αυτό το λόγο είναι απαραίτητη η διασφάλιση της εμπιστευτικότητας της χρήσης και η αποφυγή της διασποράς των πληροφοριών αυτών σε μη εξουσιοδοτημένους χρήστες.[1] Οι πληροφορίες γύρω από το ιστορικό υγείας, όπως οι ασθένειες, τα νοσήματα και η περίθαλψη που έχει λάβει κάποιος είναι από τις πλέον ευαίσθητες και εμπιστευτικές.

Ο ηλεκτρονικός φάκελος υγείας αποτελεί έναν φάκελο φροντίδας υγείας (ή υποσύνολο αυτού) για όλη τη διάρκεια ζωής του ατόμου και αποθηκευμένο σε ψηφιακή μορφή, με στόχο την υποστήριξη της συνέχειας της φροντίδας υγείας (ποιότητα, πρόσβαση, αποδοτικότητα), την εκπαίδευση και την έρευνα. Αντικαθιστά το χειρόγραφο φάκελο ως την κύρια πηγή πληροφοριών για τη φροντίδα υγείας εξασφαλίζοντας κλινικές, διοικητικές και νομικές απαιτήσεις.[2] Τα συστήματα ηλεκτρονικού φακέλου υγείας υλοποιούνται και διατηρούνται με σκοπό τη συλλογή, αποθήκευση, ανάκτηση, επεξεργασία και διακίνηση δεδομένων που σχετίζονται με τη φροντίδα υγείας ασθενών. Στα δεδομένα αυτά συμπεριλαμβανομένων τα κλινικά, διοικητικά και οικονομικά δεδομένα.[3]

Σύμφωνα με τους ορισμούς της οδηγίας 95/46/ΕΚ της Ευρωπαϊκής Ένωσης, σχετικής με την προστασία των δεδομένων, ο όρος ευαίσθητα προσωπικά δεδομένα χρησιμοποιείται για τα δεδομένα προσωπικού χαρακτήρα και αναφέρεται σε οιεσδήποτε πληροφορίες αφορούν ένα προσδιορισμένο ή προσδιορίσιμο φυσικό πρόσωπο. Ένα προσδιορίσιμο φυσικό πρόσωπο είναι εκείνο το πρόσωπο το οποίο μπορεί να προσδιοριστεί

άμεσα ή έμμεσα ειδικότερα σε σχέση με τον αριθμό ταυτοποίησής του ή ένα ή περισσότερα στοιχεία που αφορούν τη φυσική, οργανική, διανοητική, οικονομική, πολιτιστική ή κοινωνική του ταυτότητα.[4]

Τα δεδομένα σχετικά με την υγεία του ατόμου αποτελούν μέρος της προσωπικότητας του ατόμου και όχι ιδιοκτησία του φορέα που τα συλλέγει και τα επεξεργάζεται. Έτσι η επεξεργασία των δεδομένων πρέπει να συνάδει με τις σχετικές διατάξεις για την προστασία των προσωπικών ευαίσθητων δεδομένων και του ιατρονοσηλευτικού απορρήτου.[5]

Ιστορική αναδρομή σχετικά με την προστασία προσωπικών δεδομένων

Οι πρώτες αντιδράσεις στο πεδίο της προστασίας προσωπικών δεδομένων σε διεθνές επίπεδο καταγράφονται από τότε που εμφανίστηκε η ανάγκη νομοθετικής προστασίας της ιδιωτικότητας. Η ανάγκη της ιδιωτικότητας διατυπώθηκε στη Σύμβαση της Ρώμης της 4ης Νοεμβρίου 1950 για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών.

Η Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) του 1950 προστατεύει στο άρθρο 8 την ιδιωτική ζωή, στην οποία συγκαταλέγονται και τα προσωπικά δεδομένα. Ως προς τα ιατρικά δεδομένα το Δικαστήριο των Ανθρωπίνων Δικαιωμάτων όρισε αυστηρές προϋποθέσεις για την ανακοίνωσή τους σε τρίτους. Οι πρώτες ανησυχίες για την ιδιωτικότητα τέθηκαν στον νόμο για την προστασία δεδομένων του 1970 (Hesse Data Protection Act 1970), το Σουηδικό νόμο για την προστασία των δεδομένων του 1973 (Swedish Privacy Act 1973) και το νόμο περί ιδιωτικότητας των ΗΠΑ του 1974 (US Privacy Act 1974), οι οποίοι έθεσαν τις απαιτήσεις, χωρίς όμως να έχουν καμία εξουσία γύρω από την προστασία των δεδομένων.[6]

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) ήταν ο δεύτερος διεθνής οργανισμός που το 1980 ασχολήθηκε με την προστασία προσωπικών δεδομένων, εκδίδοντας «Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων». Οι αρχές αυτές περιλαμβάνουν την αρχή της περιορισμένης συγκέντρωσης και συλλογής δεδομένων, την αρχή της ποιότητας των δεδομένων, την αρχή του προσδιορισμένου σκοπού, την αρχή της περιορισμένης χρήσης των προσωπικών δεδομένων, την αρχή μέτρων ασφαλείας των προσωπικών δεδομένων, την αρχή της διαφάνειας, την αρχή της συμμετοχής του ατόμου και την αρχή της ευθύνης. Είναι ένα πλαίσιο γενικών αρχών χωρίς δεσμευτικό χαρακτήρα που συγκέντρωσε για μεγάλο διάστημα τη συναίνεση πολλών χωρών και κυρίως εκείνων που στερούνταν ειδικής νομοθεσίας για την προστασία προσωπικών δεδομένων.[7]

Σε απόλυτη συνοχή και συνάφεια με τις διεθνείς συνθήκες βρίσκεται η Διακήρυξη της Χιλιετίας των Ηνωμένων Εθνών, όπου η υπεράσπιση των ανθρωπίνων ελευθεριών, η προστασία των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα κρίνεται κεφαλαιώδους σημασίας μέσω του καθορισμού κατευθυντήριων αρχών που προσδιορίζουν τη νομιμότητα της επεξεργασίας αυτής.[8]

Νεότερα δεοντολογικά κείμενα αποτρέπουν τους γιατρούς από το να αποθηκεύουν τα προσωπικά στοιχεία των ασθενών σε ηλεκτρονικούς υπολογιστές ή αν αυτό συμβαίνει, να γίνεται κάτω από αυστηρές προϋποθέσεις. Τέτοια κείμενα είναι η Διακήρυξη της Ευρωπαϊκής Ένωσης των Γενικών Γιατρών για το Ιατρικό Απόρρητο (1979), η Απόφαση της Παγκόσμιας Ιατρικής Ένωσης για τη χρήση των Ηλεκτρονικών Υπολογιστών στην Ιατρική (1983) και η Διεθνής Συνδιάσκεψη Ιατρικών Συλλόγων, που επεξεργάστηκε τις Αρχές της Ευρωπαϊκής Ιατρικής Δεοντολογίας (1987). Τη διαφύλαξη των ιατρικών αρχείων με ατομική ευθύνη των γιατρών και την προστασία απορρήτου ακόμα και από τον εργοδότη τους και τη διοίκηση, προστατεύουν άλλα δύο κείμενα Διεθνών Οργανώσεων, ο Χάρτης του Μισθωτού Γιατρού και ο Χάρτης του Νοσοκομειακού Γιατρού, που υιοθετήθηκαν από τη Γενική Συνέλευση της Διαρκούς Επιτροπής των Γιατρών της ΕΟΚ το 1984 και το 1985, αντίστοιχα.[9]

Διεθνή και Ευρωπαϊκά νομικά εργαλεία προστασίας προσωπικών δεδομένων από την ηλεκτρονική τους διαχείριση

Σύσταση 108 του Συμβουλίου της Ευρώπης– Council of Europe Convention 108[6,10]

Η Σύσταση 108 του Συμβουλίου της Ευρώπης για την προστασία των ατόμων από την αυτόματη επεξεργασία των προσωπικών τους δεδομένων, δημιούργησε τις πρώτες διασφαλίσεις που πρέπει να τηρούνται σε σχέση με την επεξεργασία των προσωπικών δεδομένων. Η Σύσταση 108 του Συμβουλίου της Ευρώπης του 1981 ορίζει στο άρθρο 6 ότι, για την προστασία των ατόμων

από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα ιατρικά δεδομένα δεν μπορούν να γίνουν αντικείμενο αυτοματοποιημένης επεξεργασίας χωρίς εγγυήσεις για την προστασία τους, ενώ τα κριτήρια για τις εγγυήσεις πρέπει να ορίζονται με νόμο.

Η Σύσταση 108 έθεσε κανόνες για την προστασία των προσωπικών δεδομένων στην περίπτωση διασυνοριακής ροής πληροφοριών. Υπήρξε το πρώτο διεθνές δεσμευτικό κείμενο αλλά δεν ήταν άμεσης εφαρμογής. Η ισχύς της στο εσωτερικό δίκαιο των χωρών εξαρτιόταν από την κύρωσή της αλλά και τη θέσπιση εσωτερικών ρυθμίσεων. Η Σύσταση 108 άρχισε να ισχύει στην Ελλάδα από την 01/01/1995, χωρίς ωστόσο να δημιουργεί ένα επαρκές καθεστώς προστασίας των προσωπικών δεδομένων.

Πρόταση R (81)1 του Συμβουλίου της Ευρώπης– Council of Europe Recommendation R(81)1[6,11]

Το συμβούλιο της Ευρώπης ανέπτυξε την οδηγία R(81)1 που έδινε ακριβείς οδηγίες για τη χρήση των αυτοματοποιημένων ιατρικών βάσεων δεδομένων, κάτι για το οποίο δεν είχε παρατηρηθεί μέχρι τότε το αντίστοιχο διεθνές ενδιαφέρον. Η οδηγία R(81)1 απαίτησε από τις ιατρικές βάσεις δεδομένων να αναπτύξουν ένα σύνολο από κανονισμούς που θα καθοδηγούν όλες τις λειτουργίες και καθόρισε ένα ελάχιστο μέγεθος περιεχομένου που πρέπει να αναφέρεται σε κάθε αναπτυσσόμενο κανονισμό για τη νέα βάση ιατρικών δεδομένων κάτι που περιγράφεται ως πολιτική ασφαλείας.

Πρόταση R (75)5 του Συμβουλίου της Ευρώπης– Council of Europe Recommendation R (75)5[6,12]

Το έργο του Συμβουλίου της Ευρώπης στην περιοχή της ιατρικής γενετικής και της βιοηθικής οδήγησε στην άποψη ότι ίσως υπάρξουν κάποια προβλήματα ανάμεσα στις απαιτήσεις για συμβουλευτική σε θέματα γενετικής και στην προστασία των δεδομένων που ανταλλάσσονται, με αποτέλεσμα την αναθεώρηση της Πρότασης για τις Αυτοματοποιημένες Τράπεζες Ιατρικών δεδομένων. Αυτό το έργο ήταν μια προσπάθεια να καταγραφεί η κατάσταση της παροχής υγείας στην Ευρώπη και να διασφαλιστεί ότι οι επαγγελματίες υγείας ακολουθούν τα πρότυπα κατά τη διαχείριση των ιατρικών δεδομένων έτσι ώστε οι ασθενείς να μπορούν να είναι σίγουροι ότι τα προσωπικά τους δεδομένα προστατεύονται με ένα ομοιόμορφο τρόπο. Αυτή η νέα Πρόταση υιοθετήθηκε στις 12 Φεβρουαρίου 1997 ως Πρόταση R (75)5 και αντικατέστησε τη μέχρι τότε ισχύουσα προσφέροντας μια νέα βάση για τον τρόπο διαχείρισης ιατρικών προσωπικών δεδομένων συμπεριλαμβάνοντας και τα προσωπικά δεδομένων γύρω από τη γενετική.

Οδηγία της Ευρωπαϊκής Ένωσης 95/46/ΕΚ[6,13]

Στα κράτη-μέλη της Ευρωπαϊκής Ένωσης σταθμό στην προστασία των προσωπικών δεδομένων αποτελεί η Οδηγία 95/46/ΕΚ για την «προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα» και για την «ελεύθερη κυκλοφορία των δεδομένων» αυτών. Με την Οδηγία αυτή εξασφαλίζεται η εναρμόνιση των εθνικών νομοθεσιών των κρατών-μελών ως προς την προστασία των προσωπικών δεδομένων και η ελεύθερη κυκλοφορία τους στα κράτη-μέλη. Η οδηγία της Ευρωπαϊκής Ένωσης 95/46/ΕΚ υιοθετήθηκε στις 24 Οκτωβρίου 1995. Η θέση της είναι αρκετά διαφορετική από το σύμφωνο και τις μέχρι τώρα προτάσεις του Συμβουλίου της Ευρώπης στο ότι η οδηγία είναι υποχρεωτική για όλες τις χώρες της Ευρωπαϊκής Ένωσης. Ωστόσο, η θέση της περιορίζεται στην νόμιμη ισχύ και αρμοδιότητα του Ευρωπαϊκού Νόμου σε κάθε κράτος-μέλος.

Healh Insurance Portability and Accountability Act, HIPAA (Δράση φορητότητας και υπευθυνότητας ασφάλειας υγείας)

Το Αμερικανικό Κογκρέσο θέσπισε τη Δράση Φορητότητας και Υπευθυνότητας Ασφάλειας Υγείας (Health Insurance Portability and Accountability Act, HIPAA) το 1996 για να περιορίσει τη δυνατότητα των εργοδοτών να αρνηθούν ασφαλιστική κάλυψη στους εργαζομένους με προϋπάρχοντα προβλήματα υγείας. Αυτός ο νόμος είχε ως αποτέλεσμα τη διασφάλιση της ιδιωτικότητας του ασθενή αλλά και την αύξηση του κόστους παροχής φροντίδας υγείας. Ως HIPAA περιγράφηκε μια αρχή προστασίας του καταναλωτή που εκτός των άλλων δίνει στα άτομα το δικαίωμα να λάβουν τον προσωπικό ηλεκτρονικό τους φάκελο, να ζητήσουν τροποποιήσεις στον φάκελο τους και να μάθουν σε ποιους αποκαλύφτηκαν πληροφορίες από τον φάκελο τους.

Τα πρότυπα ασφάλειας της HIPAA ισχύουν για τις προστατευμένες ιατρικές πληροφορίες που είτε αποθηκεύονται είτε μεταφέρονται ηλεκτρονικά. Προστατευμένες είναι αυτές οι πληροφορίες που οδηγούν στην

αναγνώριση της ταυτότητας του ασθενούς δηλαδή τα ευαίσθητα προσωπικά δεδομένα.[14]

Στην Αμερική το 2003 θεσμοθετήθηκε η νομική υποχρέωση της προάσπισης της ιδιωτικότητας και της εμπιστευτικότητας των δεδομένων του ασθενή υπό την αιγίδα του HIPAA. Οι κανονισμοί HIPAA θέτουν τις αρχές και τις διαδικασίες για την εξασφάλιση ότι η αποκάλυψη προσωπικών δεδομένων θα μειωθεί στο ελάχιστο δυνατό για την εκπλήρωση του σκοπού για τον οποίο τα προσωπικά δεδομένα αποκαλύφθηκαν

Σύμφωνα με τις νομοθετικές ρυθμίσεις της HIPAA, οι ιατρικές πληροφορίες δεν πρέπει να αποκαλύπτονται χωρίς τη συγκατάθεση του ασθενή, εκτός εάν απαιτείται η αποκάλυψη τους κάτω από ειδικές συνθήκες, όπως για ερευνητικούς σκοπούς. Η συναίνεση που απαιτείται για την αποκάλυψη των προσωπικών πληροφοριών του ασθενή εξαρτώνται από την αιτία της αποκάλυψής τους. Έτσι για την αποκάλυψη πληροφοριών, οι οποίες είναι απαραίτητες για τον καθορισμό της θεραπείας, της χρέωσης και της κάλυψης των υπηρεσιών για την παροχή φροντίδας του ατόμου, απαιτείται μια απλή, γενική συναίνεση από τον ίδιο τον ασθενή.[16]

Η HIPAA απαιτεί από τα νοσοκομεία να έχουν μηχανισμούς για να μπορεί να ελέγχεται ποιο άτομο είχε πρόσβαση και σε ποια δεδομένα, την ημερομηνία και την ώρα που έγινε αυτό, εάν η πρόσβαση ήταν επιτυχής και κατά ποιο τρόπο έγινε αυτό, δηλαδή εάν απλά είδε τα δεδομένα, εάν έγραψε νέα, εάν έκανε αλλαγές ή εάν έσβησε κάποια δεδομένα. Οι απαιτήσεις είναι οι ίδιες και σε δεδομένα που δεν είναι σε μορφή κειμένου αλλά σε μορφή εικόνας (αξονική-μαγνητική-ακτινογραφία). Έτσι θέτει περιορισμούς στη χρήση των εικόνων και αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε αυτές.[15,17]

Ελληνική πραγματικότητα και θεσμικό πλαίσιο ασφαλείας

Η Συνταγματική κατοχύρωση της προστασίας προσωπικών δεδομένων

Κατά την τελευταία αναθεώρηση του Συντάγματος κρίθηκε επιβεβλημένη η κατοχύρωση ενός νέου, ειδικού δικαιώματος προστασίας των προσωπικών δεδομένων. Το νέο άρθρο 9Α του ελληνικού Συντάγματος 1975/86/01 που συμπεριλήφθηκε στο Σύνταγμα με την τελευταία αναθεώρηση του 2001 ορίζει ότι ο «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών δεδομένων, όπως ο νόμος ορίζει». Στη νέα διάταξη αναδεικνύεται ωστόσο η σοβαρότητα των κινδύνων που εμπεριέχει η επεξεργασία δεδομένων με ηλεκτρονικά μέσα. Η προστασία προσωπικών δεδομένων ανήκει στην κατηγορία των νέων δικαιωμάτων που κατοχυρώνει το αναθεωρημένο Σύνταγμα, κοινό στοιχείο των οποίων είναι η εξασφάλιση του πολίτη όχι μόνο έναντι της κρατικής εξουσίας αλλά και έναντι των ιδιωτών. Η μόνη απόφαση του αναθεωρητικού νομοθέτη σχετικά με τις εγγυήσεις προστασίας των προσωπικών δεδομένων αφορά τη Συνταγματική κατοχύρωση της ανεξάρτητης αρχής με αποστολή τη διασφάλιση του δικαιώματος. Η ίδρυση ανεξάρτητων αρχών αποτυπώνεται ως εγγενές χαρακτηριστικό του συστήματος προστασίας προσωπικών δεδομένων σε διεθνή κείμενα, δεσμευτικά ή μη.[18,19]

Ο Νόμος 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα[19]

Ο ελληνικός νόμος 2472/97 μεταφέρει την Κοινοτική Οδηγία στο εσωτερικό δίκαιο και συγχρόνως εκπληρώνει την υποχρέωση της Ελλάδας που απορρέει από τη Σύσταση 108 του Συμβουλίου της Ευρώπης να θεσπίσει ειδικές διατάξεις για την προστασία των προσωπικών δεδομένων. Σύμφωνα με την Ευρωπαϊκή Οδηγία 95/46/ΕΚ –και τον Ελληνικό νόμο 2472/97– η επεξεργασία των ιατρικών δεδομένων υπόκειται σε ειδικές ρυθμίσεις.

Η προστασία των ιατρικών δεδομένων διέπεται από τις διατάξεις Ν. 2472/97 και Ν. 2774/99 και τις διατάξεις σχετικά με το ιατρικό απόρρητο. Σύμφωνα με το νόμο 2472/97, ο ασθενής του οποίου τα ευαίσθητα δεδομένα υπόκεινται κάποιας μορφής επεξεργασία από κάποιους έχει το δικαίωμα:

- Να ενημερωθεί για τις πληροφορίες που τον αφορούν και αποτελούν αντικείμενο αρχειοθέτησης
- Να μάθει το σκοπό της επεξεργασίας, ποιοι θα έχουν πρόσβαση στα δεδομένα και πόσο χρόνο θα διαρκέσει η επεξεργασία
- Να ζητήσει τη διόρθωση, την προσωρινή μη χρήση, τη μη διαβίβαση μέρους ή όλων των δεδομένων.

Οι υποχρεώσεις των υπευθύνων για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι οι εξής:

- Να γνωστοποιήσουν στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα τη σύσταση και λειτουργία αρχείου, αποτελούμενου από ευαίσθητα δεδομένα ασθενών ή την έναρξη της επεξεργασίας τους, ενώ σε μερικές περιπτώσεις απαιτείται και σχετική άδεια
- Οι παραπάνω ενέργειες πρέπει να γίνονται εντός συγκεκριμένης προθεσμίας, όπως αυτή ορίζεται από την Αρχή. Η πάροδος της προθεσμίας αυτής συνεπάγεται σοβαρές διοικητικές κυρώσεις που επιβάλλει η Αρχή αλλά και ποινικές, που διώκονται αυτεπάγγελτα ή ύστερα από παρέμβαση της Αρχής
- Οι υποχρεώσεις των υπευθύνων της επεξεργασίας ισχύουν και αφορούν όλες τις επεξεργασίες δεδομένων προσωπικού χαρακτήρα και όλα τα αρχεία ανεξάρτητα εάν αυτά ανήκουν σε ιδιωτικούς ή δημόσιους χώρους υγείας
- Σε περίπτωση παράβασης ο υπεύθυνος υπόκειται στις κυρώσεις του νόμου ανάλογα βέβαια με τον χαρακτήρα και το μέγεθος της παράβασης ανεξάρτητα από τη φύση του αρχείου.

ΕΠΙΛΟΓΟΣ

Ο καθορισμός των ηθικών αλλά και νομικών διαδικασιών και κριτηρίων όσο αφορά στην ηλεκτρονική συλλογή, επεξεργασία και διακίνηση προσωπικών ευαίσθητων δεδομένων σε πιθανούς δευτερεύοντες χρήστες δεδομένων υγείας, όπως είναι οι ασφαλιστικές και φαρμακευτικές εταιρείες είναι απαραίτητος. Διαφορετικά τίθεται σε κίνδυνο τόσο η σχέση επαγγελματιών υγείας – ασθενούς αλλά πιθανόν και αυτή των μελών της κοινωνίας, αφού ο ασθενής, ίσως από το φόβο αποκάλυψης πληροφοριών σε τρίτους, να μην εμπιστευθεί κρίσιμες πληροφορίες που αφορούν όχι μόνο στην υγεία του αλλά και στη διατήρηση της δημόσιας υγείας.[20,21,22]

Μέσα στο νοσοκομείο, όπου πολυάριθμες ειδικότητες και εξειδικεύσεις συνυπάρχουν, κανείς από τους συμμετέχοντες στη λειτουργία του δεν μπορεί να ικανοποιήσει τις ανάγκες του σε πληροφόρηση χωρίς τη συμπληρωματική πληροφόρησή του. Ο καθένας έχει την ανάγκη να πληροφορείται και να πληροφορεί. Κάθε δυσλειτουργία στη ροή της πληροφορίας δημιουργεί έλλειμμα και περιορισμό δυνατοτήτων στην άσκηση του έργου του. Ο βαθμός και η ποιότητα της ενημέρωσης και της επικοινωνίας επιδρούν στη διαμόρφωση των σχέσεων του προσωπικού υγείας με τον ασθενή και καθορίζουν την ποιότητα της θεραπευτικής σχέσης.[23]

Οι επαγγελματίες υγείας καθώς επίσης και οι επαγγελματίες πληροφορικής υγείας είναι σημαντικό να γνωρίζουν ότι πρέπει να σέβονται την ιδιωτικότητα των ασθενών και ότι κάθε ρήγμα σε αυτή λόγω της χρήσης προσωπικών δεδομένων των ασθενών χωρίς τη συγκατάθεσή τους αποτελεί απειλή. Επαγρύπνηση, συνεχής έλεγχος, ευαισθητοποίηση των χρηστών και λήψη κατάλληλων, αποδοτικών, λογικών και οικονομικά ανεκτών μέτρων είναι μερικά από τα απαραίτητα μέτρα για να διασφαλιστεί η τήρηση του ιατρονοσηλευτικού απορρήτου, να εξασφαλιστεί η εμπιστευτική χρήση των προσωπικών ευαίσθητων δεδομένων χωρίς να θίγεται η αυτονομία και η αυτοδιάθεση του ατόμου.[20]

Η εφαρμογή πολιτικής ασφαλείας για τα πληροφοριακά συστήματα σε ένα οργανισμό όπως το νοσοκομείο αποτελεί νομική υποχρέωση για το ίδιο αφού πρέπει να ικανοποιεί τις απαιτήσεις για την προστασία των ευαίσθητων προσωπικών δεδομένων που βρίσκονται αποθηκευμένα στο ιατρικό ηλεκτρονικό του φάκελο όπως αυτές διατυπώνονται στον Νόμο 2472 του 1997 για την «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».[7]

Η κατάσταση γίνεται ακόμη πιο περίπλοκη και κρίνεται επιτακτικότερη η εφαρμογή της με τη συμμετοχή ανεξάρτητων οργανισμών υγείας στην ανταλλαγή ηλεκτρονικών φακέλων υγείας καθώς μέχρι τώρα η υλοποίηση παγκόσμιας πολιτικής ασφαλείας αποτελεί απλά ένα φιλόδοξο σχέδιο.[24]

Η δημιουργία εμπιστοσύνης είναι προαπαιτούμενο για την ανάπτυξη της κοινωνίας της πληροφορίας. Οι πολίτες προτιμούν υπηρεσίες και πληροφορίες προσαρμοσμένες στις ανάγκες και τις απαιτήσεις τους, γνωρίζοντας ότι προστατεύεται το δικαίωμά τους στην ιδιωτική ζωή.[25]

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Fernandez EB, Larrondo PM. *Security Models for Medical and Genetic Information Systems: Requirements for Access Control*. LACCET 04. Proceedings of the 2nd International Latin American and Caribbean Conference for Engineering and Technology "Challenges and Opportunities for Engineering Education, Research and Development" 2004 Jun 2–4, Miami, Florida, USA
2. Computer-based Patient Record Institute. Work Group on CP Description. *Computer-based Patient Record description of Content*. Bethesda, MD: Computer-based Patient Record Institute, May 1996:5
3. Work Group on Computerization of Patient Records. *Report to the Secretary of the US Department of Health and*

Human Services. Toward a National Health Information Infrastructure. Chicago: American Hospital Association, April 1993:5
4. Αποστολάκης Ι. *Θέματα Διοίκησης Πληροφοριακών Υποδομών στις Μονάδες Υγείας*. Εκδόσεις MediForce, Αθήνα: 2005
5. Πάγκαλος Γ, Μαυρίδης Ι. *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων*. Εκδόσεις Ανικούλα, Θεσσαλονίκη: 2002
6. Barber B. Patient data and security: an overview. *Int J Med Inform* 1998, 49:19–30
7. Κάτσικας Σ, Γκρίτζαλης Δ, Γκρίτζαλης Σ. *Ασφάλεια Πληροφοριακών Συστημάτων*. Εκδόσεις Νέων Τεχνολογιών, Αθήνα: 2004
8. Ελληνική Εταιρεία Επιστημόνων Ηλεκτρονικών Υπολογιστών και Πληροφορικής. *Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα*. Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 1995
9. Μαλλιαρού Μ. *Πολιτική ασφαλείας και διασφάλιση ιατρικού απορρήτου ηλεκτρονικού φακέλου υγείας ασθενών*. Μεταπτυχιακή Διπλωματική Εργασία Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών, Τμήμα Νοσηλευτικής, Διαπανεπιστημιακό Διατμηματικό πρόγραμμα μεταπτυχιακών σπουδών: Ειδίκευση Πληροφορικής Υγείας, Αθήνα 2006
10. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Council of Europe Convention 108, 1981 Jan, ISBN (1982) 92871–00225
11. Council of Europe *Recommendation, R(81)1, on Automated Medical Data Banks*, Council of Europe, Strasbourg, 1981 Jan 23
12. Council of Europe *Recommendation, R(97)5, on The Protection of Medical Data*, Council of Europe, Strasbourg, 1997 Feb13
13. Council of Europe, *Directive 95/46/EC*. On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, Strasbourg, 1995
14. Kibbe DC. Ten Steps to HIPAA Security Compliance. *Fam Pract Manag* 2005, 12:43–49
15. Zhou Z, Liu BJ. HIPAA compliant auditing system for medical images. *Comp Med Imag Graph* 2005, 29:2–3
16. Κρητικάκη Σ. *Ασφάλεια ιατρικών δεδομένων και ηλεκτρονικός φάκελος ασθενών*. Μεταπτυχιακή Διπλωματική Εργασία Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών. Τμήμα Νοσηλευτικής. Διατμηματικό πρόγραμμα μεταπτυχιακών σπουδών. Ειδίκευση Πληροφορικής Υγείας. Αθήνα, 2001
17. Fodor J. "HIPAA and the EHR: Making Technical Safeguard Changes". *J AHIMA* 2004, 75:54–55
18. Κοσμόπουλος Α. *Η πολιτική ασφαλείας στο σύγχρονο νοσοκομείο*. Παρουσίαση στο 1ο Πανελλήνιο Συνέδριο για την Υγεία & τα Προσωπικά Δεδομένα. 2006 Μάρτιος 28-29, Αθήνα: Εθνικό Ίδρυμα Ερευνών
19. Κατσάνος Π. *Διαχείριση ευαίσθητων δεδομένων ασθενών στο διαδίκτυο*. Μεταπτυχιακή Διπλωματική Εργασία Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών. Τμήμα Νοσηλευτικής. Διατμηματικό πρόγραμμα μεταπτυχιακών σπουδών. Πληροφορική Υγείας. Αθήνα, 2002
20. Fairweather NB, Rogerson S. A moral approach to electronic patient records. *Med Inform* 2001, 26:219–234
21. Harman LB. Ethical challenges in the management of health information. In: Harman LB (ed) *Ethical challenges in the management of health information*. Gaithersburg, Aspen, 2001
22. Harman LB. Professional code of ethics and values. In: Harman LB editor. *Ethical challenges in the management of health information*. Gaithersburg, Aspen, 2001
23. Σαρρής Μ, Χρυσάκης Μ, Σούλης Σ, Γεωργιάδου Μ. Επικοινωνία και διαχείριση πληροφορίας στις υπηρεσίες υγείας: από τον ιατρικό φάκελο στον φάκελο φροντίδας υγείας. *Νοσηλευτική* 2002, 41:174–184
24. Defteraios S, L ambrinoudakis C, Gritzalis D. High level security policies for health: from theory to practice. *Stud Health Technol Inform* 2004, 103:416–423
25. COM(2005) 356 τελικό Ανακοίνωση της επιτροπής, στο Ευρωπαϊκό Κοινοβούλιο, στην Ευρωπαϊκή οικονομική και κοινωνική επιτροπή και στην επιτροπή περιφερειών. Βρυξέλλες, 30/4/2004 ηλ-υγεία (ηλεκτρονική υγεία) – βελτίωση των υπηρεσιών ιατροφαρμακευτικής περίθαλψης για τους πολίτες της Ευρώπης: Σχέδιο δράσης για έναν Ευρωπαϊκό Χώρο Ηλ-Υγείας

Υποβλήθηκε: 25/01/2007
Επανυποβλήθηκε: 26/02/2008
Εγκρίθηκε: 05/05/2008