



Θέματα Προστασίας Προσωπικών Δεδομένων

- ερσος, σύστημα ηλεκτρονικής συνταγογράφησης -

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Ζ. Καρδασιάδου, Γ. Παναγοπούλου, Τμήμα Ελεγκτών



ErSOS: ελληνικό τμήμα του ευρωπαϊκού πιλοτικού προγράμματος

Άδεια για επεξεργασία ευαίσθητων δεδομένα υγείας ασθενών

Υπεύθυνος επεξεργασίας: Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης («εθνικό σημείο επαφής») (NCP)

- **Τήρηση αρχείων καταγραφής** στα οποία περιέχεται **ο κωδικός ταυτοποίησης του ασθενή** (περιλαμβάνουν και την ταυτοποίηση του φαρμακείου) το οποίο εκτελεί την ιατρική συνταγή μέσω του προγράμματος erSOS.
- **Εκτελών την επεξεργασία:** φαρμακεία της Αθήνας (μέλη της ΦΑΡΜΑΞΙΣ), στην πιλοτική φάση του erSOS (εισαγωγή των στοιχείων αναγνώρισης του ασθενούς, λήψη και τήρηση έγγραφης συγκατάθεσης του ασθενούς



Όροι σχετικά με την προστασία προσωπικών δεδομένων

Νομική βάση για την επεξεργασία ευαίσθητων δεδομένων υγείας: συγκατάθεση του ασθενούς

Συγκατάθεση

- **Εγγράφως προς το ΑΠΘ για την τήρηση των αρχείων καταγραφής**
Φυλάσσεται ασφαλώς από το φαρμακείο για λογαριασμό του υπευθύνου επεξεργασίας.
- **Εγγράφως εξειδίκευση της αρχικής συγκατάθεσης** που έχει δώσει ο ασθενής στο φορέα παροχής υπηρεσιών υγείας της χώρας προέλευσης, για την πρόσβαση του συγκεκριμένου φαρμακείου στα δεδομένα του



Δικαίωμα ενημέρωσης, πρόσβασης υποκειμένων

- επαρκής **πληροφόρηση** στα υποκείμενα των δεδομένων σχετικά με την επεξεργασία τους μέσω του epSOS (π.χ μέσω ειδικής ιστοσελίδας, ειδικού εντύπου)
- δυνατότητα **πρόσβασης** στα πλήρη στοιχεία που τηρούνται για αυτούς από το ΑΠΘ.

Χρόνος τήρησης προσωπικών δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα, που τηρούνται στα αρχεία καταγραφής, **τηρούνται μόνον για το χρονικό διάστημα του έργου.**

Μετά το πέρας του χρόνου αυτού καταστρέφονται με ασφαλή τρόπο σύμφωνα με το αρ. 10 παρ. 2 του ν. 2472/1997 και την Οδηγία 1/2005 της Αρχής.



Μέτρα ασφάλειας

Ο υπεύθυνος επεξεργασίας οφείλει να τηρεί τους όρους του άρθρου 10 του ν. 2472/1997 σχετικά με το απόρρητο και την ασφάλεια της επεξεργασίας προσωπικών δεδομένων.

Η πολιτική ασφάλειας που τηρούν τα «εθνικά σημεία επαφής» του epSOS κατά την πιλοτική φάση έχει οριστεί από το epSOS (epSOS Baseline Security Policy), και ο υπεύθυνος επεξεργασίας δεσμεύεται να την τηρεί.

Περιλαμβάνονται οργανωτικά, διοικητικά και τεχνικά μέτρα τα οποία έχουν οριστεί από το epSOS σε ευρωπαϊκό επίπεδο και εφαρμόζονται για το σύνολο των NCP που συμμετέχουν στην πιλοτική φάση.



Η Ομάδα Εργασίας του Άρθρου 29 θα εκδώσει σύντομα **Γνώμη** σχετικά με τα θέματα προστασίας προσωπικών δεδομένων στο erSOS



Σύστημα Ηλεκτρονικής Συνταγογράφησης

Υπεύθυνος επεξεργασίας: Γενική Γραμματεία Κοινωνικών Ασφαλίσεων,
(ΥΠΕΔΥΦΚΑ και Διεύθυνση Μηχανογραφικών Εφαρμογών)

Νομική βάση : Άρθρο 7 παρ. 2 στοιχ. δ' και ε' (παροχή υπηρεσιών υγείας, δημόσιος έλεγχος κοινωνικών παροχών)

Όροι σχετικά με την προστασία προσωπικών δεδομένων

Πρόσβαση στα δεδομένα υγείας μέσω του ΣΗΣ

ΦΚΑ, φαρμακοποιοί, μονάδες παροχής υπηρεσιών υγείας και ιατροί -> πρόσβαση **μόνο στα στοιχεία της βάσης που αφορούν τον εκάστοτε ΦΚΑ ή οι ίδιοι παράγουν.**

Κατ' εξαίρεση, ο ιατρός -> πρόσβαση σε δεδομένα 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 (βλ. άρθρο 3 παρ. 8 του ν. 3892/2010).



Δικαίωμα ενημέρωσης, πρόσβασης υποκειμένων

- επαρκής πληροφόρηση στα υποκείμενα των δεδομένων σχετικά με την επεξεργασία τους μέσω του ΣΗΣ (π.χ μέσω ειδικού εντύπου, ειδικής ιστοσελίδας)
- δυνατότητα πρόσβασης στα πλήρη στοιχεία που τηρούνται για αυτούς μέσω του ΣΗΣ.

Χρόνος τήρησης προσωπικών δεδομένων

- 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.



Ασφάλεια επεξεργασίας

Μέσα σε ένα χρόνο από την ημερομηνία χορήγησης της άδειας πρέπει:

α) να εκπονηθεί **μελέτη επικινδυνότητας, πολιτική ασφάλειας και σχέδιο ασφάλειας**

Πρέπει να περιλαμβάνονται: Τα τεχνικά, διοικητικά και οργανωτικά μέτρα ασφάλειας του ΣΗΣ, Σχέδιο Έκτακτης Ανάγκης του ΣΗΣ

β) να υποβληθεί κείμενο **κώδικα δεοντολογίας** σχετικά με την προστασία των προσωπικών δεδομένων που τηρεί ο υπεύθυνος επεξεργασίας ειδικά για το προσωπικό που δεν καλύπτεται από το ιατρικό απόρρητο.



Ασφάλεια επεξεργασίας

Ειδικότερα μέτρα:

- **ασφαλής τρόπος αναγνώρισης των χρηστών** κατά την εγγραφή στο ΣΗΣ. π. χ εγγραφή των ιατρών μόνο μετά από επαλήθευση της ταυτότητάς τους και της ιδιότητάς τους ως ιατρών

- **Τήρηση αρχείων καταγραφής** για τον πλήρη έλεγχο των λεπτομερειών πρόσβασης

- το αργότερο μέχρι την επόμενη ανανέωση της άδειας (28-2-2014, *ενόψει της ανάγκης αξιολόγησης της εφαρμογής του νέου συστήματος*) : **Εφαρμογή κατάλληλων μέτρων ασφάλειας για τη διασφάλιση της ρητής και ειδικής συγκατάθεσης του ασθενούς** στις περιπτώσεις πρόσβασης ιατρού σε δεδομένα ασθενών που έχουν καταχωριστεί από άλλους ιατρούς (άρθρο 3 παρ. 8 του ν. 3892/2010 (π.χ. μέσω ηλεκτρονικής κάρτας υγεία, την οποία φέρει ο ίδιος ο ασθενής)



Σχέδιο υπουργικής απόφασης που θα ρυθμίσει επιμέρους ζητήματα (άρθρο 8 του ν. 3892/2010)

- ✓ διαδικασία και τις τεχνικές ή άλλες απαιτήσεις για την εγγραφή και ταυτοποίηση ιατρών, φαρμακοποιών και μονάδων παροχής υγείας
- ✓ οργάνωση της βάσης δεδομένων (εφαρμογή ΣΗΣ)
- ✓ τα τεχνικά και οργανωτικά μέτρα ασφάλειας των υποδομών και πληροφοριακών συστημάτων

... να υποβληθεί στην Αρχή για γνωμοδότηση