G
D
P
R

General Data Protection Regulation

Άννα Μαστοράκου

GDPR: Ορισμός και Αρχική Εισαγωγή

Το GDPR είναι ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation GDPR). Στοχεύει να προσφέρει στους πολίτες της ΕΕ μια ενιαία και εναρμονισμένη προσέγγιση όσον αφορά την προστασία της ιδιωτικής ζωής.

Επιδιώκει να ενισχύσει τα δικαιώματα των πολιτών για την προστασία των δεδομένων τους, όπως ορίζεται στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ.

Μετά από σχεδόν τέσσερα χρόνια συζήτησης και συζήτησης, το GDPR εγκρίθηκε από το κοινοβούλιο της ΕΕ στις 14 Απριλίου 2016.

GDPR: Είναι Κανονισμός ή απλή Οδηγία;

Το κοινοβούλιο της ΕΕ αποφάσισε ότι το νέο πλαίσιο προστασίας της ιδιωτικής ζωής θα δημιουργηθεί τη μορφή κανονισμού, **μιας δεσμευτικής νομοθετικής πράξης που εφαρμόζεται άμεσα σε όλα τα κράτη μέλη της ΕΕ, εξαλείφοντας την ανάγκη κατάρτισης τοπικών νομοθετικών πράξεων**. Ωστόσο, είναι πιθανό να υπάρξουν διαφορές ως προς τον τρόπο με τον οποίο ο κανονισμός ερμηνεύεται και επιβάλλεται σε διάφορα κράτη μέλη.

90% κανονισμός
10% οδηγία κατά την ενσωμάτωση στο δίκαιο της εκάστοτε χώρας – διαβούλευση σχεδίου νόμου

θα ρυθμίζει το "πως" οι επιχειρήσεις θα προστατεύουν τα Προσωπικά Δεδομένα...

των Ευρωπαίων πολιτών. Μικρές, μεσαίες και μεγάλες επιχειρήσεις...

πρέπει να προσαρμοστούν προκειμένου ν'αποφύγουν τα σκληρά πρόστιμα.

Οι βασικές αλλαγές που φέρνει η οδηγία **GDPR**, είναι:

#1. Τα στοιχεία πρέπει να διατηρούνται ανώνυμα, για προστασία της ιδιωτικότητας

#2. Απαιτείται η συγκατάθεση του πελάτη για την επεξεργασία των δεδομένων του

#3. Σε περίπτωση παραβίασης **(hacking)**, απαιτείται η άμεση ενημέρωση του πελάτη

#4. Απαιτείται η ασφαλής διακίνηση των δεδομένων, εκτός των ορίων της ΕΕ

#5. Σε μεγάλες επιχειρήσεις απαιτείται η ύπαρξη Ειδικού Φύλαξης Δεδομένων **(DPO)**

Η **GDPR** υποχρεώνει, τη προσαρμογή σε μια βασική πρακτική προστασίας δεδομένων...

για τη λήψη, διαχείριση και επεξεργασία τους, καθώς...

και την μετακίνηση των προσωπικών δεδομένων, εκτός των ορίων της ΕΕ.

Η **GDPR** μεγιστοποιεί την προστασία και των Ευαίσθητων Προσωπικών Δεδομένων.

Γιατί ;

Η παγκοσμιοποίηση δημιούργησε μία ανεξέλεγκτη τεράστια δεξαμενή προσωπικών δεδομένων

Τα συστήματα πληροφορικής στην υγεία αποτελούν στρατηγική προτεραιότητα κάθε αναπτυγμένης κοινωνίας

Κ.Ι.Δ. – Ν 3418 / 2005

Άρθρο 13

Ιατρικό απόρρητο

1. Ο ιατρός οφείλει να τηρεί αυστηρά απόλυτη εχεμύθεια για οποιοδήποτε στοιχείο υποπίπτει στην αντίληψή του ή του αποκαλύπτει ο ασθενής ή τρίτοι, στο πλαίσιο της άσκησης των καθηκόντων του, και το οποίο αφορά στον ασθενή ή τους οικείους του.

2. Για την αυστηρή και αποτελεσματική τήρηση του ιατρικού απορρήτου, ο ιατρός οφείλει:

α) να ασκεί την αναγκαία εποπτεία στους βοηθούς, στους συνεργάτες ή στα άλλα πρόσωπα που συμπράττουν ή συμμετέχουν ή τον στηρίζουν με οποιονδήποτε τρόπο κατά την άσκηση του λειτουργήματός του και

β) να λαμβάνει κάθε μέτρο διαφύλαξης του απορρήτου και για το χρόνο μετά τη με οποιονδήποτε τρόπο παύση ή λήξη άσκησης του λειτουργήματός του.

3. Η άρση του ιατρικού απορρήτου επιτρέπεται όταν:

α) Ο ιατρός αποβλέπει στην εκπλήρωση νομικού καθήκοντος. Νομικό καθήκον συντρέχει, όταν η αποκάλυψη επιβάλλεται από ειδικό νόμο, όπως στις περιπτώσεις γέννησης, θανάτου, μολυσματικών νόσων και άλλες, ή από γενικό νόμο, όπως στην υποχρέωση έγκαιρης αναγγελίας στην αρχή, όταν ο ιατρός μαθαίνει με τρόπο αξιόπιστο ότι μελετάται κακούργημα ή ότι άρχισε ήδη η εκτέλεσή του και, μάλιστα, σε χρόνο τέτοιο, ώστε να μπορεί ακόμα να προληφθεί η τέλεση ή το αποτέλεσμά του.

β) Ο ιατρός αποβλέπει στη διαφύλαξη έννομου ή άλλου δικαιολογημένου, ουσιώδους δημοσίου συμφέροντος ή συμφέροντος του ίδιου του ιατρού ή κάποιου άλλου, το οποίο δεν μπορεί να διαφυλαχθεί διαφορετικά.

γ) Όταν συντρέχει κατάσταση ανάγκης ή άμυνας.

4. Η υποχρέωση τήρησης ιατρικού απορρήτου αίρεται, εάν συναινεί σε αυτό εκείνος στον οποίο αφορά, εκτός εάν η σχετική δήλωσή του δεν είναι έγκυρη, όπως στην περίπτωση, που αυτή είναι προϊόν πλάνης, απάτης, απειλής, σωματικής ή ψυχολογικής βίας, ή εάν η άρση του απορρήτου συνιστά προσβολή της ανθρώπινης αξιοπρέπειας.

5. Οι ιατροί που ασκούν δημόσια υπηρεσία ελέγχου, επιθεώρησης ή πραγματογνωμοσύνης απαλλάσσονται από την υποχρέωση τήρησης του ιατρικού απορρήτου μόνο έναντι των εντολέων τους και μόνο ως προς το αντικείμενο της εντολής και τους λοιπούς όρους χορήγησής της.

6. Η υποχρέωση τήρησης και διαφύλαξης του ιατρικού απορρήτου δεν παύει να ισχύει με το θάνατο του ασθενή.

Κ.Ι.Δ. – Ν 3418 / 2005

Άρθρο 14

Τήρηση ιατρικού αρχείου

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΄).

2. Τα ιατρικά αρχεία πρέπει να περιέχουν το ονοματεπώνυμο, το πατρώνυμο, το φύλο, την ηλικία, το επάγγελμα, τη διεύθυνση του ασθενή, τις ημερομηνίες της επίσκεψης, καθώς και κάθε άλλο ουσιώδες στοιχείο που συνδέεται με την παροχή φροντίδας στον ασθενή, όπως, ενδεικτικά και ανάλογα με την ειδικότητα, τα
ενοχλήματα της υγείας του και το λόγο της επίσκεψης, την πρωτογενή και δευτερογενή διάγνωση ή την αγωγή που ακολουθήθηκε.

3. Οι κλινικές και τα νοσοκομεία τηρούν στα ιατρικά τους αρχεία και τα αποτελέσματα όλων των κλινικών και παρακλινικών εξετάσεων.

4. Η υποχρέωση διατήρησης των ιατρικών αρχείων ισχύει:

α) στα ιδιωτικά ιατρεία και τις λοιπές μονάδες πρωτοβάθμιας φροντίδας υγείας του ιδιωτικού τομέα, για μία δεκαετία από την τελευταία επίσκεψη του ασθενή και

β) σε κάθε άλλη περίπτωση, για μία εικοσαετία από την τελευταία επίσκεψη του ασθενή.

5. Ο ιατρός λαμβάνει όλα τα αναγκαία μέτρα, έτσι ώστε στην περίπτωση επιστημονικών δημοσιεύσεων να μην γνωστοποιείται με οποιονδήποτε τρόπο η ταυτότητα του ασθενή στον οποίο αφορούν τα δεδομένα. Εάν, λόγω της φύσης της δημοσίευσης, είναι αναγκαία η αποκάλυψη της ταυτότητας του ασθενή ή στοιχείων που υποδεικνύουν ή μπορούν να οδηγήσουν στην εξακρίβωση της ταυτότητάς του, απαιτείται η ειδική έγγραφη συναίνεσή του.

6. Ο ιατρός τηρεί τα επαγγελματικά του βιβλία με τέτοιο τρόπο, ώστε να εξασφαλίζεται το ιατρικό απόρρητο και η προστασία των προσωπικών δεδομένων.

7. Στα ιατρικά αρχεία δεν πρέπει να αναγράφονται κρίσεις ή σχολιασμοί για τους ασθενείς, παρά μόνον εάν αφορούν στην ασθένειά τους.

8. Ο ασθενής έχει δικαίωμα πρόσβασης στα ιατρικά αρχεία, καθώς και λήψης αντιγράφων του φακέλου του. Το δικαίωμα αυτό, μετά το θάνατό του, ασκούν οι κληρονόμοι του, εφόσον είναι συγγενείς μέχρι τετάρτου βαθμού.

9. Δεν επιτρέπεται σε τρίτο η πρόσβαση στα ιατρικά αρχεία ασθενή. Κατ' εξαίρεση επιτρέπεται η πρόσβαση:

α) στις δικαστικές και εισαγγελικές αρχές κατά την άσκηση των καθηκόντων τους αυτεπάγγελτα ή μετά από αίτηση τρίτου που επικαλείται έννομο συμφέρον και σύμφωνα με τις νόμιμες διαδικασίες,

β) σε άλλα όργανα της Ελληνικής Πολιτείας, που με βάση τις καταστατικές τους διατάξεις έχουν τέτοιο δικαίωμα και αρμοδιότητα.

10. Ο ασθενής έχει το δικαίωμα πρόσβασης, σύμφωνα με τις οικείες διατάξεις, στα εθνικά ή διεθνή αρχεία στα οποία έχουν εισέλθει τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν.

Το GDPR → εισάγει ορισμούς για ειδικά δεδομένα

- Δεδομένα φυσικής ή ψυχικής υγείας
- Γενετικά, κληρονομικά δεδομένα
- Βιομετρικά χαρακτηριστικά

Αρχές κανονισμού GDPR

Δεν απαιτείται άδεια από την ΑΠΔΠΧ για την τήρηση αρχείου ΠΔ

Γνωμοδότηση από την ΑΠΔΠΧ για ειδικές περιπτώσεις

Προθεσμίες λογοδοσίας υπεύθυνου επεξεργασίας

- ✓ Αρχή νομιμότητας – ρητή έγγραφη συγκατάθεση
- ✓ Αρχή αντικειμενικότητας
- ✓ Αρχή διαφάνειας – ενημέρωση ασθενούς
- ✓ Αρχή σκοπού με τάση περιορισμού του *
- ✓ Αρχή ελαχιστοποίησης των δεδομένων
- ✓ Αρχή της ακρίβειας (διόρθωσης ή διαγραφής)
- ✓ Αρχή του περιορισμού
- ✓ Αρχή της ασφάλειας (ακεραιότητας και εμπιστευτικότητας)
- ✓ Αρχή της λογοδοσίας (ΑΠΔΠΧ) - 72 ώρες μετά το συμβάν

** Ρητή απαγόρευση παράδοσης στοιχείων σε ασφαλιστική εταιρεία, εργοδότη ή τράπεζα*

Δικαιώματα ασθενών κατά το GDPR

Ανάκληση συγκατάθεσης
Τήρηση αρχείου / προστασία – έλλειψη διαθεσιμότητας στοιχείων – παράλειψη γνωστοποίησης → πρόστιμο
Ακρίβεια και ποιότητα – εκτίμηση κινδύνου / αντικτύπου

Το GDPR αφορά όλους

- Πληροφορία έντυπη ή προφορική
- Πληροφορία ψηφιακή / ψηφιοποιημένη
- Βιολογικό υλικό ή δείγμα

Επίπεδο συμμόρφωσης / πιστοποίησης GDPR

Τυποποίηση data mapping
Τυποποιημένες διαδικασίες
Gap analysis
Risk analysis
Αξιολόγηση ;

Φύση ιατρικού έργου, πλήθος προσωπικού όγκος δεδομένων και πολυπλοκότητα

DPO
Υπεύθυνος Προστασίας Δεδομένων
Μεγάλη κλίμακα επεξεργασίας
Εκτίμηση αντικτύπου D/PIA

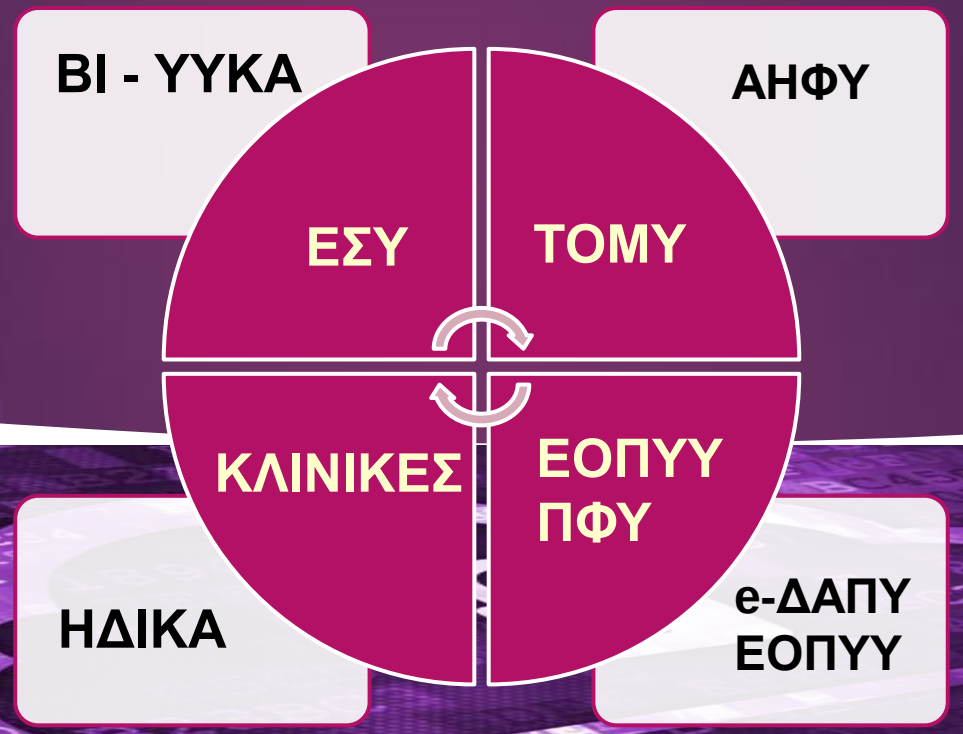
Κλινικός ιατρός
Πολυϊατρείο
Κέντρο Υγείας

Εργαστήριο
Διαγνωστικό κέντρο

Νοσοκομείο
Ιδιωτική κλινική

Πάνω από 250 άτομα προσωπικό

Ψηφιακό οικοσύστημα στην Ελλάδα



Δεν υπάρχει πιστοποίηση διαλειτουργικότητας και ασφάλειας των πληροφοριακών συστημάτων

Στρατηγικός σχεδιασμός
Κωδικοποίηση

Το GDPR → ενίσχυση της εμπιστοσύνης των πολιτών

- Νομικό πλαίσιο
- Ψηφιακή τεχνολογία ή IT
- Συμβουλευτική, σχεδιασμός, πιστοποίηση

Κόστος υλοποίησης / κόστος μη συμμόρφωσης

«Απειλή ή ευκαιρία»

Συνέπειες μη συμμόρφωσης στο GDPR

Καταγγελία → δημοσιοποίηση → Ζημιά στη φήμη

Καταγγελία → Πρόστιμο* και υποχρέωση συμμόρφωσης

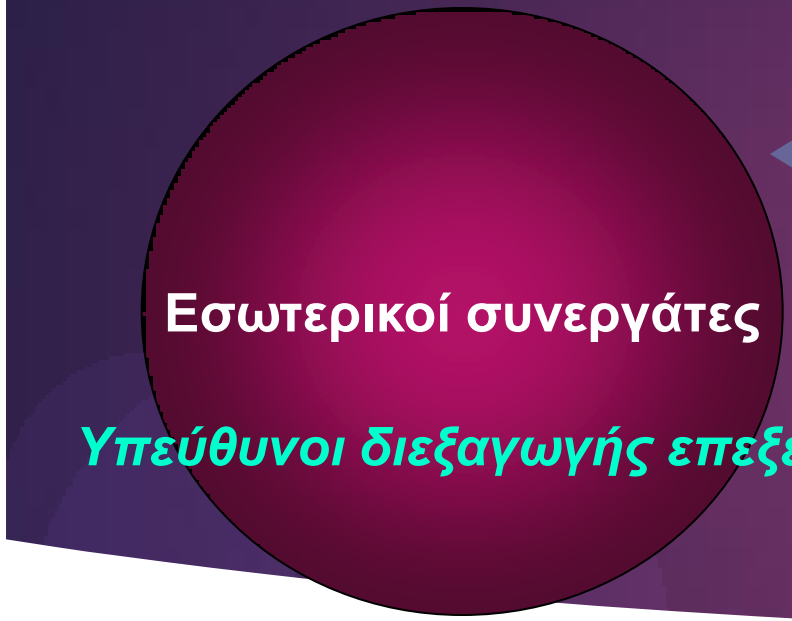
Καταγγελία → Κόστος συμμόρφωσης

- *Πρόστιμο : έως 20 εκατ ή 4% του ετήσιου τζίρου*
- *Παύση εργασιών*
- *Ασφάλιση κινδύνων πληροφορικής και διαδικτύου*

Βήματα υλοποίησης GDPR

ΑΠΔΠΧ = 40 άτομα
Μ.Κ.Ο.
Εταιρείες συμβούλων
Πέτσινο πιστοποιητικό

Σφαίρες οργάνωσης GDPR

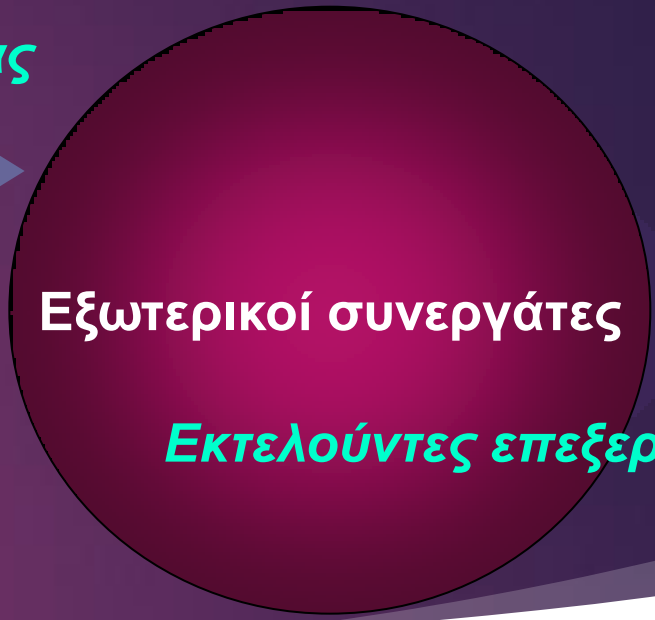


Εσωτερικοί συνεργάτες

Υπεύθυνοι διεξαγωγής επεξεργασίας

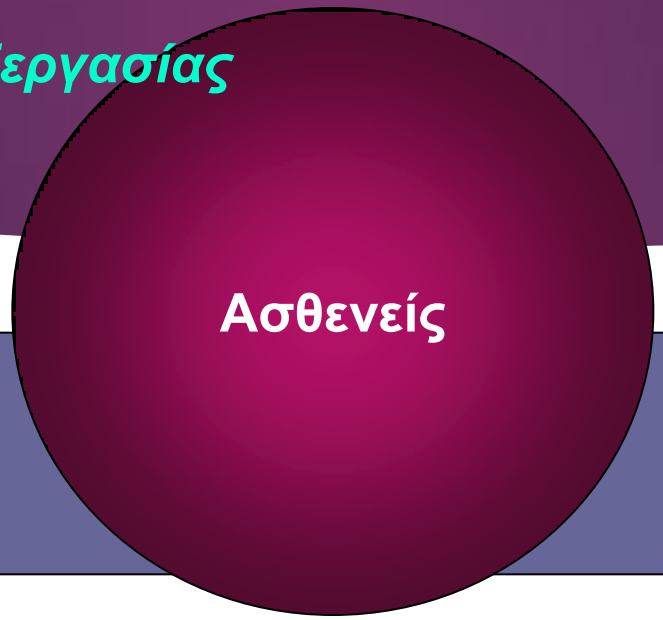
Υπεύθυνος επεξεργασίας

Γραπτή εντολή
Ρήτρες εμπιστευτικότητας
Μέτρα ασφαλείας
Συμμόρφωση



Εξωτερικοί συνεργάτες

Εκτελούντες επεξεργασία

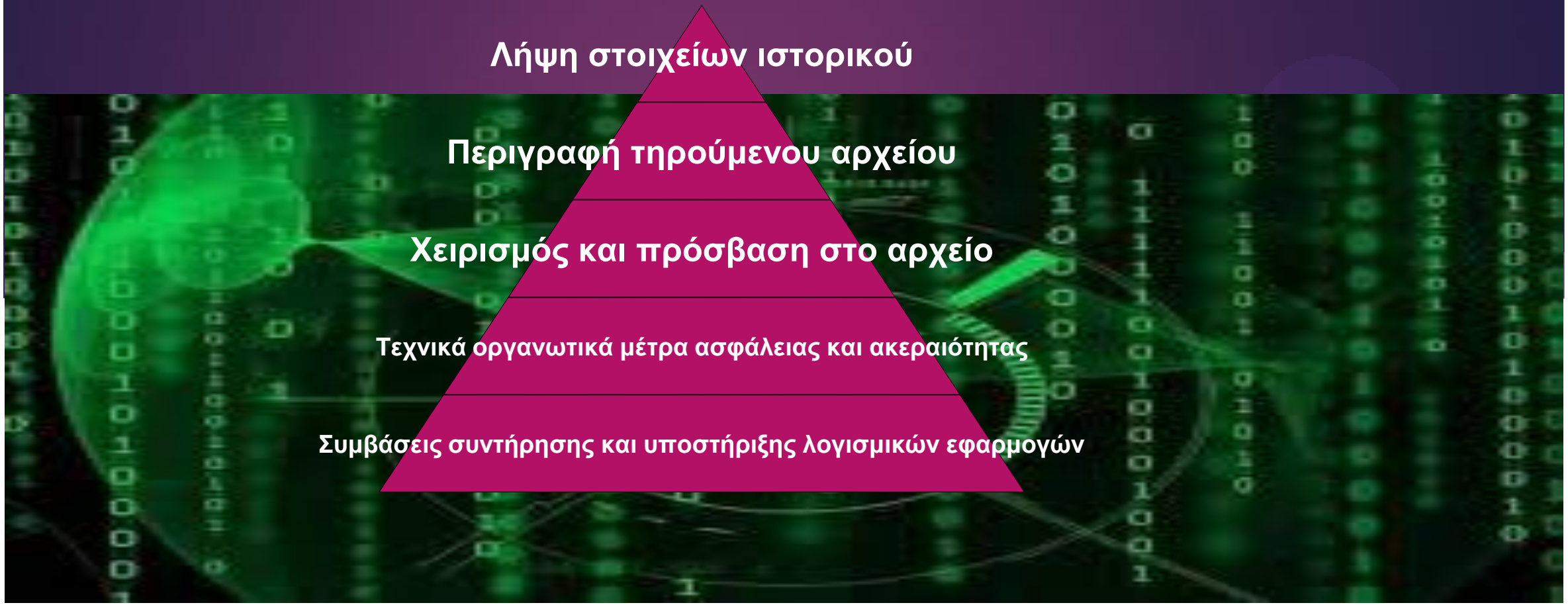


Ασθενείς

Αυτοπρόσωπη παρουσία
Χειρισμός αντιδράσεων

Αυτορρύθμιση από επαγγελματικούς / θεσμικούς φορείς – δήλωση συμμόρφωσης

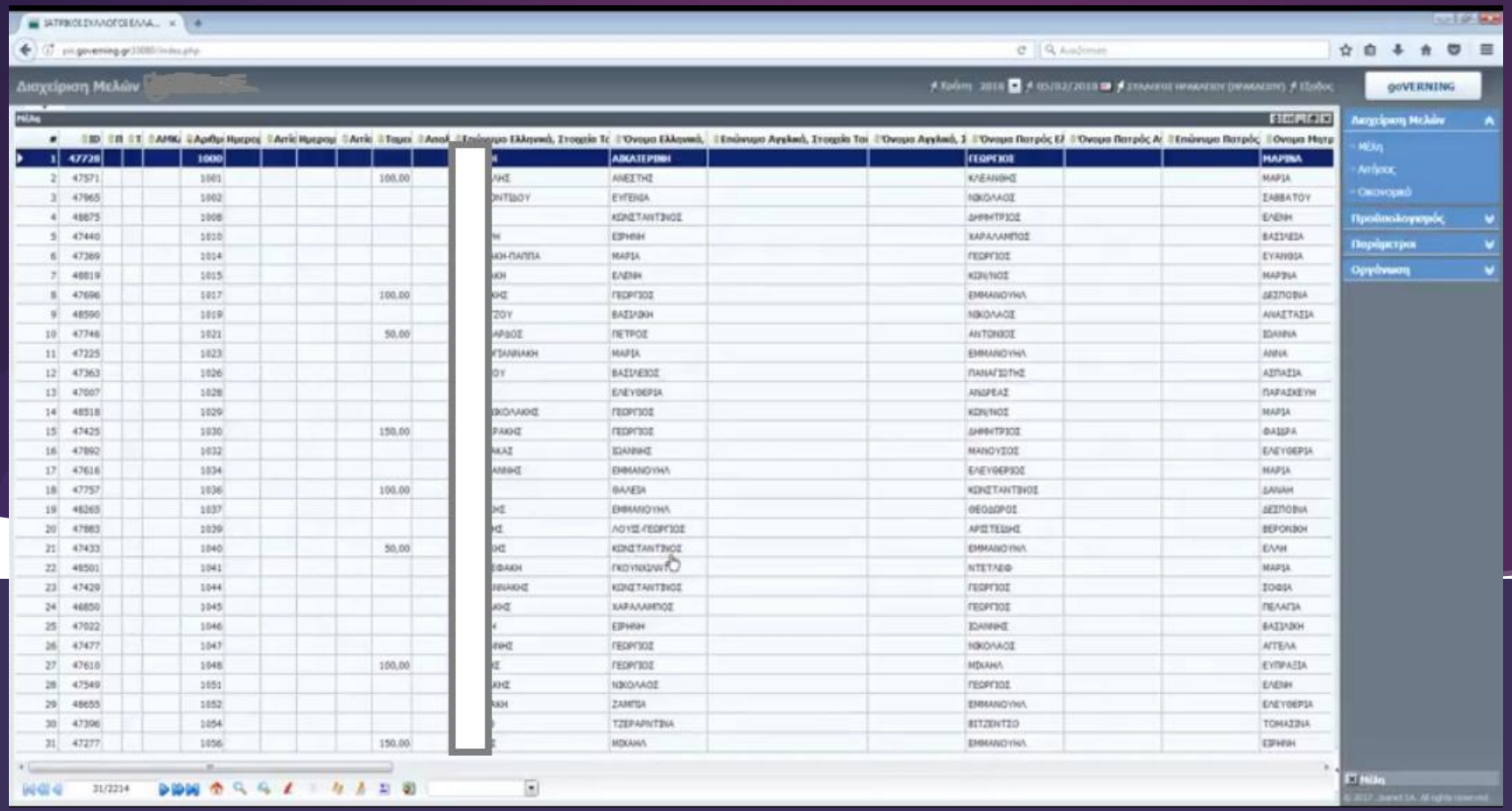
Κανόνες λήψης και τήρησης ιατρικού αρχείου



Σημεία αιχμής

1. Προφύλαξη / προστασία προσωπικών δεδομένων κατά τη λήψη ιστορικού ασθενούς
2. Ειδικό έντυπο συγκατάθεσης (σκοπός, χρόνος τήρησης και καταστροφής)
3. Φύλαξη έντυπου υλικού που περιέχει ΠΔ
4. Προστασία από ιούς και επιθέσεις, back up
5. Βιντεοσκόπηση, αρχείο
6. Ανωνυμοποίηση, κρυπτογράφηση
7. Συμβάσεις λογισμικού
8. Προσωπικό –βαθμός πρόσβασης - ρήτρες διαφύλαξης ΠΔ
9. Σωστή παράδοση αποτελέσματος – ταυτοποίηση
10. Διαδικασίες ΕΟΠΥΥ – παραπεμπτικά – μεταφορά στην Αθήνα
11. Έγκριση για έλεγχο ιστορικού ασθενούς στην ΗΔΙΚΑ
12. Διακίνηση βιολογικού υλικού
13. Προστασία έναντι κινδύνων φωτιάς κλπ
14. Διαδικασία καταστροφής έντυπων ή ηλεκτρονικών αρχείων
15. Τυποποίηση πρόσβασης σε ιατρικά δεδομένα από εκτελούντες την επεξεργασία
16. Ενημέρωση – παραλαβή αποτελέσματος από τρίτους
17. Έλεγχο ροής πληροφορίας ΠΔ σε πολυϊατρεία, Νοσοκομεία

Διασύνδεση Ιατρικών Συλλόγων με ΠΙΣ



- 50 πεδία καταγραφής
- Ονοματεπώνυμο
- ΑΜΚΑ, ΔΑΤ
- ΑΦΜ
- ΑΜ ΤΣΑΥ
- Διεύθυνση
- Τηλέφωνα
- E-mail
- Εργασία
- Ποινές
- Εκπαιδεύσεις
- Εξειδικεύσεις
- Ξένες γλώσσες
- ΕΦΚΑ
- Πληρωμές στους ΙΣ
- κλπ