
# “Ασφάλεια κρίσιμων εφαρμογών Ψηφιακής Υγείας” στο υπολογιστικό νέφος της Η.ΔΙ.Κ.Α. Α.Ε.

# Η.ΔΙ.Κ.Α. Α.Ε.

Η Η.ΔΙ.Κ.Α. Α.Ε. είναι ένας Δημόσιος Φορέας ΔΕΚΟ (Ν.3607/2007), που **σκοπό έχει** να την παροχή ολοκληρωμένων λύσεων ΤΠΕ υψηλής ποιότητας, σε Φορείς Κοινωνικής Ασφάλισης, Φορείς Κοινωνικής Πρόνοιας και Φορείς Παροχής Υγείας, **που επιτυγχάνεται** μέσω της διαλειτουργικότητας των διαφορετικών Πληροφοριακών Συστημάτων, καθώς και με τον ψηφιακό μετασχηματισμό των Φορέων Υγείας στο H-Cloud.

Με τον Ν.4727/2020 ΦΕΚ ΤΑ’ 184/23.9.20 Α.87§3, ορίζεται η Η.ΔΙ.Κ.Α. Α.Ε. ως το Κυβερνητικό Νέφος Τομέα Υγείας (H-Cloud).

# Ψηφιακός Μετασχηματισμός με έργα Ψηφιακής Υγείας στο H-Cloud

**Εθνικό Σχέδιο Ανάκαμψης & Ανθεκτικότητας «Ελλάδα 2.0»**

«Ηλεκτρονικό Σύστημα Παρακολούθησης Διακίνησης Φαρμάκων» ΗΣΠαΔιΦ

Ολοκλήρωση του «Ατομικού Ηλεκτρονικού Φακέλου Υγείας» ΑΗΦΥ

Ψηφιακός Μετασχηματισμός της υπηρεσίας «Διαχείριση της Περίθαλψης Ογκολογικών Ασθενών»

Πληροφοριακά Συστήματα «Διαχείρισης και Παρακολούθησης έργων προληπτικών εξετάσεων» και «Υπηρεσίες Call Center»

Ενοποίηση των Μητρώων Υγείας & Κοινωνικής Ασφάλισης της ΗΔΙΚΑ

Έργο ΕΣΠΑ - γέφυρα ανάμεσα στα δύο προγράμματα ΕΣΠΑ (2016-2020) & (2021-2027)

Εγκατάσταση συστημάτων RIS PACS & απομαγνητοφώνησης ιατρικών πράξεων και γνωματεύσεων Νοσοκομείων & Μονάδων ΠΦΥ

# Τι ορίζονται ως δεδομένα υγείας

- **Ιατρικά αρχεία**: Διαγνώσεις, θεραπείες, φάρμακα, εργαστηριακά αποτελέσματα, αναφορές απεικόνισης & άλλες κλινικές πληροφορίες,
- **Προσωπικά στοιχεία υγείας (PHI)**: ασφαλιστικές πληροφορίες, λεπτομέρειες τιμολόγησης, χρονοδιαγράμματα ραντεβού, ακόμη και επιλογές τρόπου ζωής που μπορεί να επηρεάσουν την υγεία,
- **Γενετικές πληροφορίες:** πληροφορίες από DNA, RNA και άλλες γενετικές αναλύσεις, που μπορεί να αποκαλύπτουν προδιαθέσεις για ασθένειες και πληροφορίες που σχετίζονται με την υγεία,
- **Δεδομένα από wearable devices**: πληροφορίες που συλλέγονται από ιχνηλάτες φυσικής κατάστασης, έξυπνα ρολόγια και άλλες φορητές συσκευές, όπως καρδιακοί παλμοί, μοτίβα ύπνου και επίπεδα δραστηριότητας,
- **Δεδομένα από Εφαρμογές Υγείας**: πληροφορίες που εισάγονται από χρήστες σε εφαρμογές υγείας, συμπεριλαμβανομένων αρχείων καταγραφής διατροφής, παρακολούθησης συμπτωμάτων και ερωτηματολογίων ψυχικής υγείας, και
- **Δεδομένα Έρευνας**: πληροφορίες που συλλέγονται για σκοπούς ιατρικής έρευνας, η οποία συχνά περιλαμβάνει de-identified ή anonymized δεδομένα ασθενών.

# Γιατί είναι ευαίσθητα τα δεδομένα υγείας

- **Ανησυχίες περί απορρήτου**: μπορεί να αποκαλυφθούν προσωπικές λεπτομέρειες σχετικά με την υγεία ενός ατόμου, **τις οποίες δεν θέλει να μοιραστούν δημόσια**,
- **Στιγματισμός**: ορισμένες καταστάσεις υγείας φέρουν κοινωνικό στίγμα, και η αποκάλυψη αυτών των πληροφοριών **θα μπορούσε να οδηγήσει σε διακρίσεις ή προκαταλήψεις**,
- **Διακρίσεις**: η πρόσβαση σε δεδομένα υγείας θα μπορούσε να χρησιμοποιηθεί για την **διάκριση εις βάρος ατόμων σε τομείς όπως η απασχόληση, η ασφάλιση, η στέγαση, ή αλλού**,
- **Κλοπή ταυτότητας**: τα δεδομένα υγείας μπορούν **να χρησιμοποιηθούν για κλοπή ή απάτη ιατρικής ταυτότητας**,
- **Βλάβη φήμης**: διαρροές πληροφοριών υγείας, **ιδιαίτερα στην περίπτωση δημοσίων προσώπων**, θα μπορούσαν να βλάψουν τη φήμη τους καθώς και την απρόσκοπτη εκτέλεση των καθηκόντων τους.

# Βασικές Αρχές Προστασίας Δεδομένων

- **Ελαχιστοποίηση δεδομένων**: συλλογή και επεξεργασία μόνο του ελάχιστου όγκου δεδομένων που είναι απαραίτητος για έναν συγκεκριμένο σκοπό,
- **Περιορισμός Σκοπού**: τα δεδομένα θα πρέπει να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς, και να μην χρησιμοποιούνται για άλλους σκοπούς χωρίς συγκατάθεση ή νομική βάση,
- **Διαφάνεια:** τα άτομα θα πρέπει να ενημερώνονται για τον τρόπο συλλογής, χρήσης και διαμοιρασμού των δεδομένων τους,
- **Ακρίβεια**: τα δεδομένα πρέπει να είναι ακριβή και να διατηρούνται ενημερωμένα,
- **Περιορισμός αποθήκευσης**: τα δεδομένα πρέπει να αποθηκεύονται μόνο για όσο χρονικό διάστημα είναι απαραίτητο για τον καθορισμένο σκοπό,
- **Ακεραιότητα και εμπιστευτικότητα**: τα δεδομένα πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, τροποποίηση ή καταστροφή,
- **Λογοδοσία**: υποχρέωση απόδειξης της συμμόρφωσης με την λήψη μέτρων προστασίας δεδομένων,
- **Νομιμότητα, Δικαιοσύνη και Διαφάνεια**: η επεξεργασία πρέπει να γίνεται σύμφωνα με τους νόμους, δίκαια και με διαφάνεια.

# Επιχειρησιακές προκλήσεις ασφάλειας των εφαρμογών Ψηφιακής Υγείας

| Διαθεσιμότητα | Συμμόρφωση | Προστασία δεδομένων |
|---|---|---|

Οι πλατφόρμες των υπηρεσιών ψηφιακής υγείας της χώρας πρέπει να είναι διαθέσιμες ανά πάσα στιγμή

Ευθύνη των Οργανισμών για τη διασφάλιση των GDPR και NIS2 καθώς και άλλα κοινά πρωτόκολλα ανταλλαγής δεδομένων εντός της ΕΕ

Αποτροπή εισβολέων που στοχεύουν τις εφαρμογές ψηφιακής υγείας με σκοπό να πάρουν πρόσβαση σε ευαίσθητα δεδομένα

# Διαθεσιμότητα υπηρεσιών και δεδομένων Ψηφιακής Υγείας

## Διαθεσιμότητα

- **Το H-CLOUD φιλοξενείται και αναπτύσσεται σε τρία ευρωπαϊκά Data Centers ενός από τους μεγαλύτερους παρόχους υπηρεσιών pubic-cloud, ο οποίος:**
  - Εξασφαλίζει ανθεκτικότητα και υψηλή διαθεσιμότητα όλων των παρεχόμενων υπηρεσιών CLOUD,
  - Εξασφαλίζει μια ολοκληρωμένη στρατηγική επιχειρηματικής συνέχειας και αποκατάστασης από καταστροφές,
  - Αυξάνει την ανθεκτικότητα και διαθεσιμότητα των πληροφοριακών συστημάτων παρέχοντας 99,99% uptime SLA για εικονικές μηχανές και υπηρεσίες as-a-Service,
  - Κάνει εξοικονόμηση κόστους και ενέργειας λειτουργίας των Πληροφοριακών Συστημάτων έναντι της λειτουργίας αυτών σε on-premises υποδομές, και
  - Ικανοποιεί τις ανάγκες συμμόρφωσης των κανονιστικών ρυθμίσεων για κρίσιμες εφαρμογές.

# Συμμόρφωση στο κανονιστικό πλαίσιο

## Συμμόρφωση

- **Οργανωτικά μέτρα Ασφάλειας Πληροφοριών της Η.ΔΙ.Κ.Α. Α.Ε.:**
  - Γραφείο «Προστασίας Δεδομένων» (DPO).
  - Γραφείο «Ασφάλειας Πληροφοριών».
  - Γενική Διεύθυνση «Ψηφιακών Υποδομών»,
    - Διεύθυνση «Υποδομών»,
      - Τμήμα «Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων & Δικτύου».
- **Διοικητικά μέτρα Ασφάλειας Πληροφοριών της Η.ΔΙ.Κ.Α. Α.Ε. :**
  - Πολιτικές: Πολιτική Ασφαλείας, Πολιτική Προστασία Δεδομένων, Πολιτική Cookies, κ.α.
  - Ορισμός **«ΥΑΣΠΕ**» και «Ομάδας Αντιμετώπισης Περιστατικών» - ΟΑΠ Ασφαλείας,
  - Αυτόματη απόκριση περιστατικών: Incident Response Playbooks, Dashboard & Visualizations, AI,
  - SIEM-SOC και Managed Security Services.

# Τεχνικά Μέτρα Προστασίας των Πληροφοριακών Συστημάτων Ψηφιακής Υγείας

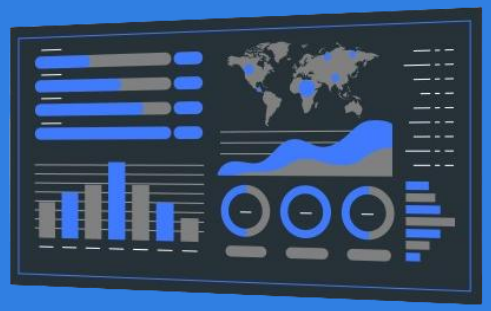
## Προστασία δεδομένων

**Στο H-Cloud έχουν ενεργοποιηθεί οι ακόλουθες CLOUD υπηρεσίες για την προστασία των Πληροφοριακών Συστημάτων Ψηφιακής Υγείας:**

- Ενεργοποίηση **Cloud Native Application Protection Platform (CNAPP)** όπως:
  - Cloud **Security Posture Management** (CSPM) & **Cloud Infrastructure Entitlement Management** CIEM)
  - Cloud **Workload Protection**
  - Cloud **Storage Protection**
  - Cloud **Key Vault Protection**
  - Cloud **Security for Containers**
  - Cloud **Security for Resource Manager**
  - Cloud **Security for Databases**
  - Cloud **Security for WebApp & API Services**
  - Cloud **Virtual Machine Security Enhancements** (+ **File Integrity Monitoring** - **FIM**)
- Ενεργοποίηση **Cloud Security Information Event Management (SIEM),** καθώς και **Cloud Security Orchestration, Automation and Response (SOAR),**
- Παροχή Υπηρεσιών **Security Operations Center (SOC)** & **Managed Security Services.**

# Σημεία ενδιαφέροντος

Διαρκής Βελτιστοποίηση των on-Prem Υποδομών Ασφαλείας



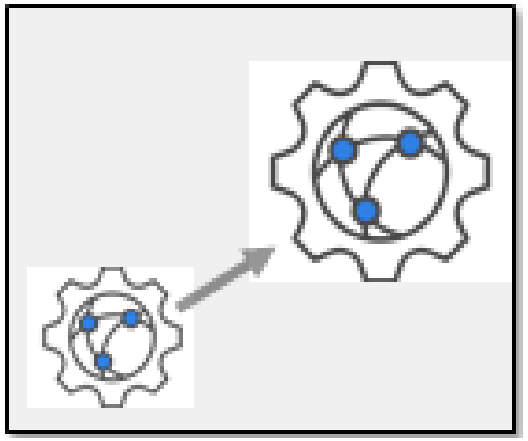
Διαρκής Βελτιστοποίηση των λειτουργιών ασφάλειας

Ασφάλεια ανθρώπων, διαδικασιών και δεδομένων

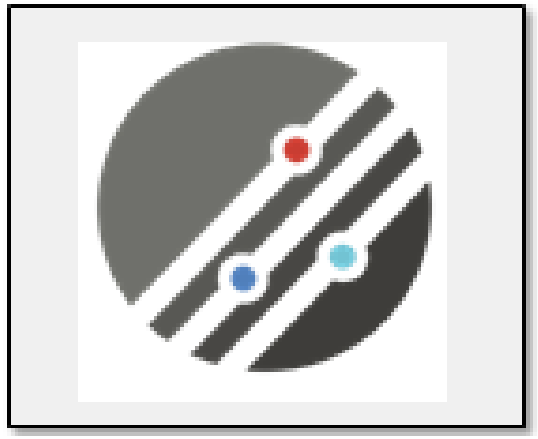
# Βέλτιστες πρακτικές κυβερνοασφάλειας Οργανισμών & Χρηστών δεδομένων Υγείας

- Η **τήρηση κρυπτογραφημένων αντιγράφων ασφαλείας** των δεδομένων υγείας των οργανισμών & μονάδων υγείας, μπορούν να μετριάσουν τους κινδύνους απώλειας των δεδομένων τους,
- Τα **προγράμματα ευαισθητοποίησης και κατάρτισης των χρηστών** Πληροφοριακών Συστημάτων Υγείας, μπορούν να διαδραματίσουν ρόλο στον μετριασμό των επιθέσεων κοινωνικής μηχανικής, και ηλεκτρονικού phishing,
- Η **τακτική σάρωση ευπαθειών** για τον εντοπισμό και την αντιμετώπιση των τρωτών σημείων - ειδικά εκείνων των συσκευών των που έχουν πρόσβαση στο Διαδίκτυο, περιορίζουν την επιφάνεια μιας κυβερνοεπίθεσης,
- Οι **τακτικές ενημερώσεις λογισμικών και λειτουργικών συστημάτων των συσκευών**, ειδικά εκείνων που έχουν πρόσβαση στο Διαδίκτυο στις πιο πρόσφατες εκδόσεις τους, περιορίζουν την επιφάνεια μιας κυβερνοεπίθεσης,
- Θα πρέπει να ακολουθούνται οι **βέλτιστες πρακτικές πολυπαραγωντικού (MFA) ελέγχου ταυτότητας** της πρόσβασης των χρηστών των Πληροφοριακών Συστημάτων ψηφιακής υγείας σε δεδομένα υγείας,
- Η **δημιουργία και τήρηση βασικών σχεδίων αντιμετώπισης περιστατικών ασφαλείας στον κυβερνοχώρο**, διασφαλίζουν ότι δεν θα επηρεαστεί η φροντίδα των ασθενών (σχέδια έκτακτης ανάγκης σε κάθε τμήμα ή υπηρεσία των οργανισμών, βελτιωμένα κανάλια επικοινωνίας, αλλά και φροντίδα της ψυχικής και σωματική ευεξίας των χρηστών),
- Η **δέσμευση των ανώτερων στελεχών των Οργανισμών** είναι καίριας σημασίας, ειδικά τώρα που η οδηγία NIS2 (**Ν.5160/2024**) **εισάγει υποχρεώσεις για την ανώτατη διοίκηση των οργανισμών**.

# Ατενίζοντας το Μέλλον



Διαρκής Αναβάθμιση της Ασφάλειας έναντι αναδυόμενων απειλών



Εξερεύνηση και εφαρμογή πρόσθετων λύσεων Security Fabric

Σχεδιασμός και επέκταση εφαρμογής hybrid architecture

Επαναξιολόγηση της στρατηγικής hybrid cloud security

# Διακρίσεις της Η.ΔΙ.Κ.Α. σε Cybersecurity

- **AI & DATA AWARDS 2025** (27/02/2025):
  - **Silver** στην κατηγορία **Best Use of AI/Data for Cybersecurity and Fraud Prevention,** για το έργο **N**ational **E**lectronic **H**ealth **R**ecord (Εθνικό Ηλεκτρονικό Μητρώο Υγείας).

- **Cyber Security Awards 2025** (5/3/2025):
  - **Κορυφαίο Βραβείο: Cyber Security Team of the Year.**

  - στην **Ενότητα 1. Cyber-Security Projects per Industry Sector:**
    - στην κατηγορία **Healthcare: Silver** για **Ενισχυμένη κυβερνοασφάλεια με Security Copilot,**
  - στην **Ενότητα 2. Cyber-Security Projects per Solution:**
    - στην κατηγορία **AI/Machine Learning Security: Gold** για **Ενισχυμένη κυβερνοασφάλεια με Security Copilot,**
  - στην **Ενότητα 3. Cyber-Security Products & Services:**
    - στην κατηγορία **Cloud Security: Gold** για **ΗΣΠαΔιΦ – SaaS WAF**

# Ευχαριστώ για την προσοχή σας

Γεώργιος Τζώρτζης,
MSc Data Communication Systems

Προϊστάμενος Τμήματος Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων & Δικτύου

Διεύθυνση Υποδομών,
Γενική Διεύθυνση Ψηφιακών Υποδομών

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Λυκούργου 10 (Νέα Διεύθυνση)
105 51, Αθήνα
T: +30.213 2168 166
F: +30.213 2168 164
M:
E: g.tzortzis@idika.gr
W: www.idika.gr