ΠΜΣ Έρευνα και Καινοτομία στις Επιστήμες Υγείας

1ος Κύκλος | 2023-2024

ΤΜΗΜΑ ΙΑΤΡΙΚΗΣ
ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

B4. Πιστοποίηση Ποιότητας και Αξιολόγηση Τεχνολογιών Υγείας

Νομικό και Κανονιστικό Πλαίσιο Ιδιωτικότητας

(GDPR, HIPAA)

Γεώργιος Δροσάτος
Εντεταλμένος Ερευνητής
Ινστιτούτο Επεξεργασίας του Λόγου, Ερευνητικό Κέντρο Αθηνά
https://www.drosatos.info

Παρασκευή 26 Απριλίου 2024

στο τέλος αυτού του μαθήματος …

Θα μπορείτε να

- Να γνωρίζετε τη νομοθεσία σχετικά με την προστασία των προσωπικών δεδομένων στο χώρο της υγεία
- Να αναγνωρίζετε την νομοθεσία σχετικά με το GDPR και το HIPAA
- Να αναγνωρίζετε τις κύριες διαφορές μεταξύ GDPR και HIPAA
- Να γνωρίζετε κάποια ενδεικτικά μέτρα συμμόρφωσης με το GDPR και HIPAA

Περιεχόμενα

1| GDPR vs. HIPAA με μια ματιά

How Does GDPR Compare to HIPAA?

- GDPR and HIPAA are two distinct sets of regulations that have contributed to a greater sense of security and privacy, particularly in the realm of information and data protection

The General Data Protection Regulation (GDPR)

- Enacted by the European Parliament, the European Commission, as well as the Council of the European Union on April 27, 2016, and went into effect on May 25, 2018
- GDPR replaced a previously enacted **data protection act**
- It is designed to **consolidate data privacy laws across Europe**
- **Aim**: protect the data security of all EU citizens
- Reimagine the way companies and industries across Europe approach data collection and security
- GDPR is considered to be one of the most significant changes in data privacy regulation in twenty years

GDPR is composed of 91 articles

7 key points

- Individual consent is required before any data can be collected or processed
- Individuals will be notified promptly if their data is breached or interfered with
- All data will be made and remain anonymous
- International data transfers will be managed more securely
- Companies are required to appoint a data protection officer (DPO) to protect client data
- Any company that provides a service or product to residents of the EU is required to comply with the GDPR
- Companies that do not comply with the GDPR regulations will be subject to hefty fines

Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA is an American law that was enacted in 1996.
- Designed to protect sensitive medical information that is electronically transferred and received.
- Initially created to **help patients retain proper insurance** in the case of job loss or change.
- HIPAA decreases medical cost by allowing healthcare administrators to use electronic documentation and records, which are more secure and more efficient than paper documentation.
- HIPAA was regulated and continues to be enforced by the United States Department of Health and Human Services.

HIPAA and HITECH and ARRA

- The Health Information Technology for Economic and Clinical Health Act (HITECH) is a subset of the **American Recovery and Reinvestment Act (ARRA) of 2009**
- HITECH act broadened the scope of what HIPAA
- expanded the privacy and security protections offered under the act by increasing legal actions available for non-compliance
- Systems affected by HIPAA laws are required to **notify patients of any data breach** and are subject to substantial fines and penalties for violations

Privacy requirements under HIPAA

- Patient identity and social security number
- Patient diagnosis and condition
- Record of care or treatment provided to a patient
- Payment information that could potentially be used to identify the patient

HIPAA vs. GDPR: Sum Up

HIPAA

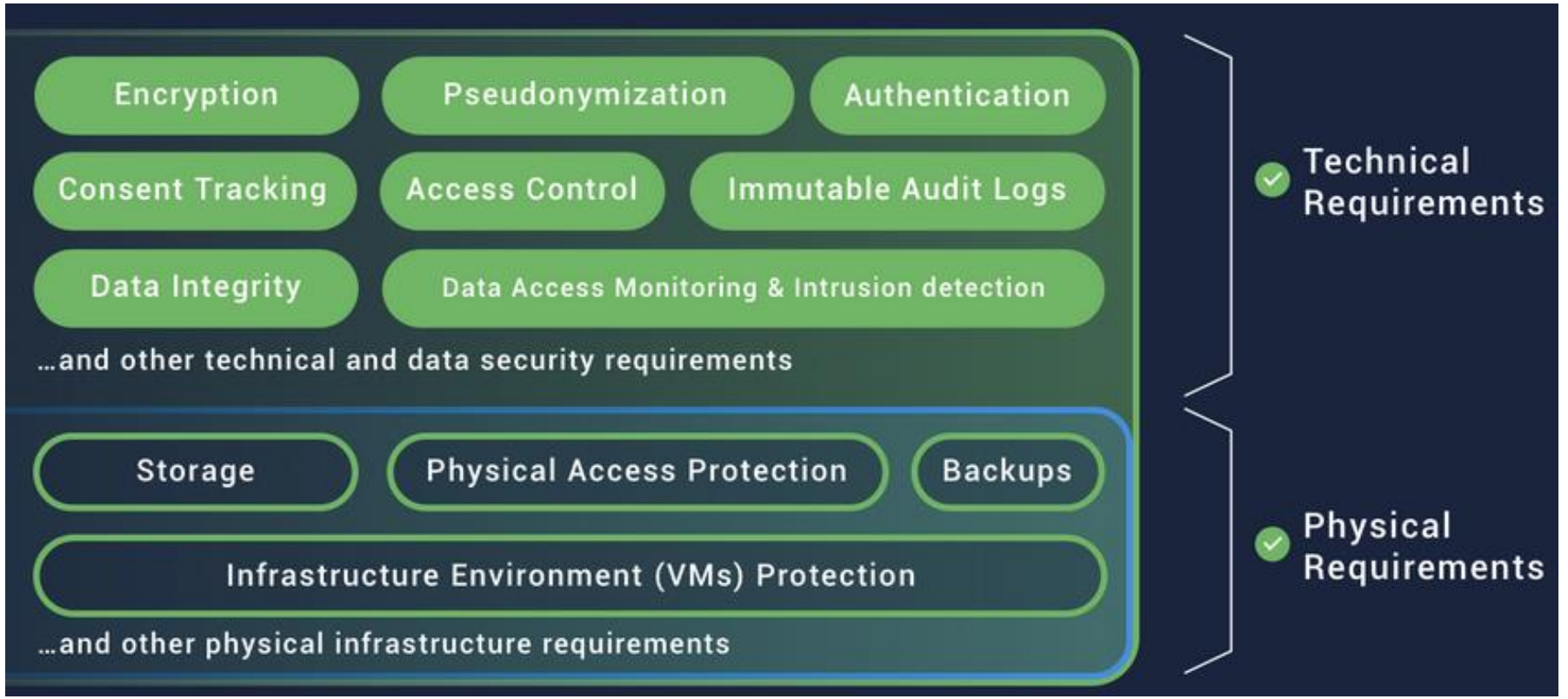
- Confidentiality, integrity, and availability of all **e-PHI***
- Protect the integrity of the information
- Protect against unauthorized disclosures
- Ensure compliance

GDPR

- Confidentiality, integrity, and availability of all **PII****
- **Data Portability**
- Store only for Consent Duration
- Privacy by Design and by Default
- Breach notification in 72 hours

* *Protected Health Information*
** *Personal Identifiable Information*

Privacy Technical and Physical Requirements



2| Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

Σκοπός και πεδίο εφαρμογής

- Να δημιουργήσει ένα **εναρμονισμένο νομικό πλαίσιο** στην Ε.Ε. σχετικά με την προστασία προσωπικών δεδομένων
- Αφορά στην, **εν όλω ή εν μέρει, αυτοματοποιημένη** επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη **μη αυτοματοποιημένη** επεξεργασία τέτοιων δεδομένων

Δεδομένα προσωπικού χαρακτήρα
(σύμφωνα με το κανονισμό)

- Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο ένα φυσικό πρόσωπο («υποκείμενο των δεδομένων»)
  - το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε **αναγνωριστικό στοιχείο ταυτότητας**, όπως **όνομα**, σε **αριθμό ταυτότητας**, σε **δεδομένα θέσης**, σε **επιγραμμικό αναγνωριστικό ταυτότητας** ή σε έναν ή περισσότερους παράγοντες που προσδιορίζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου

Παραδείγματα

- Ταυτότητα (αρ. ταυτότητας), δεδομένα ταυτότητας (ονοματεπώνυμο)
- Διεύθυνση κατοικίας
- Οικογενειακή κατάσταση, συνήθειες διαβίωσης
- Επαγγελματική ζωή: CV, εκπαίδευση, επαγγελματική κατάρτιση, βραβεία
- Χρηματοοικονομικές πληροφορίες: εισόδημα, οικονομική κατάσταση, φορολογική κατάσταση
- IP διευθύνσεις, διευθύνσεις email (name.surname@company.com), advertising ID
- Δεδομένα θέσης: ταξίδια, δεδομένα GPS, GSM data

Δεδομένα που ΔΕΝ είναι προσωπικά

- Αριθμός μητρώου εταιρίας;
- Διεύθυνση email του τύπου info@company.com;
- Ανωνυμοποιημένα δεδομένα

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα

- **δεδομένα που αποκαλύπτουν:**
  - φυλετική ή εθνοτική καταγωγή
  - πολιτικά φρονήματα
  - θρησκευτικές ή φιλοσοφικές πεποιθήσεις
  - συμμετοχή σε συνδικαλιστική οργάνωση

- **γενετικά δεδομένα, βιομετρικά δεδομένα, ή που αφορούν**
  - την υγεία,
  - τη σεξουαλική ζωή
  - τον γενετήσιο προσανατολισμό

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα

- **ΑΠΑΓΟΡΕΥΕΤΑΙ Η ΕΠΕΞΕΡΓΑΣΙΑ ΤΟΥΣ ΕΚΤΟΣ ΚΑΙ ΑΝ** μεταξύ άλλων
  - έχει δοθεί **ρητή** συγκατάθεση για έναν ή περισσότερους συγκεκριμένους σκοπούς
  - τα δεδομένα **έχουν προδήλως δημοσιοποιηθεί** από το υποκείμενο των δεδομένων
  - είναι απαραίτητη για **λόγους δημοσίου συμφέροντος**
  - είναι απαραίτητη για σκοπούς **προληπτικής ή επαγγελματικής ιατρικής**

Ποιους αφορά ο ΓΚΠΔ;

- Επεξεργασία προσωπικών δεδομένων από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία
  - **εγκατεστημένο στην ΕΕ**
    - ανεξαρτήτου τοποθεσίας επεξεργασίας
  - μη εγκαταστημένο στην ΕΕ
    - **υποκειμένων που βρίσκονται στην ΕΕ** εάν αφορά
      - προσφορά αγαθών ή υπηρεσιών – ανεξαρτήτου πληρωμής
      - παρακολούθηση της συμπεριφοράς τους – όταν λαμβάνει χώρα εντός της ΕΕ
    - σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου

Αρχές που διέπουν την επεξεργασία (1/4)

- **νομιμότητά, αντικειμενικότητα και διαφάνεια**
  - σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο
- **περιορισμός του σκοπού**
  - συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς
  - δεν υποβάλλονται σε περαιτέρω επεξεργασία

Αρχές που διέπουν την επεξεργασία (2/4)

- **ελαχιστοποίηση των δεδομένων**
  - κατάλληλα, συναφή και περιορίζονται στο αναγκαίο
- **ακρίβεια**
  - ακριβή και επικαιροποιημένα δεδομένα
  - λαμβάνονται μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων

Αρχές που διέπουν την επεξεργασία (3/4)

- **περιορισμός της περιόδου αποθήκευσης**
  - για το διάστημα που απαιτείται για τους σκοπούς επεξεργασίας
  - ή παραπάνω για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς
- **ακεραιότητα και εμπιστευτικότητα**
  - προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά

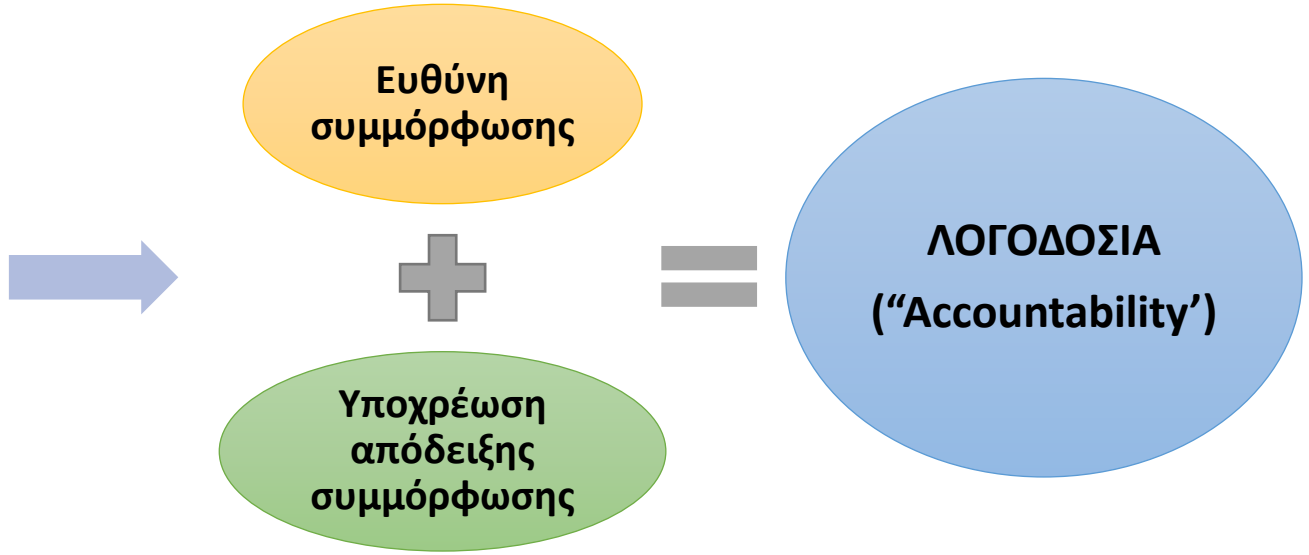
Αρχές που διέπουν την επεξεργασία (4/4)

Ο υπεύθυνος επεξεργασίας

φέρει την ευθύνη και θα πρέπει να είναι σε θέση

να αποδείξει τη συμμόρφωση

με τα προηγούμενα



Αρχείο δραστηριοτήτων επεξεργασίας

Μορφή

- Έγγραφο
- Ηλεκτρονικό
- Στη διάθεση της Εποπτικής Αρχής κατόπιν αιτήματος
- Υποχρεωτικό και για τον Εκτελούντα για τις επεξεργασίες που διεξάγει εκ μέρους του υπευθύνου επεξεργασίας

Περιεχόμενο

- Όνομα &Στοιχεία επικοινωνίας υπευθύνου επεξεργασίας/εκπροσώπου του/DPO
- Σκοποί επεξεργασίας
- Κατηγορίες υποκειμένων & προσωπικών δεδομένων
- Κατηγορίες αποδεκτών δεδομένων
- Διαβιβάσεις εκτός ΕΕ & εγγυήσεις αυτών
- Προθεσμίες διαγραφής ει δυνατόν
- Περιγραφή τεχνικών και οργανωτικών μέτρων ασφαλείας ει δυνατόν

Νομιμότητα επεξεργασίας

- **Συναίνεση** του υποκειμένου για **συγκεκριμένους σκοπούς**
- Εκτέλεση **σύμβασης**
  - ή και για τη λήψη μέτρων πριν τη σύναψη αυτής
- **Έννομη υποχρέωση του υπευθύνου επεξεργασίας**
- **Διαφύλαξη ζωτικού συμφέροντος** του υποκειμένου
  - ή άλλου φυσικού προσώπου
- Εκπλήρωση καθήκοντος προς το **δημόσιο συμφέρον**
  - ή κατά την άσκηση δημόσιας εξουσίας
- **Έννομα συμφέροντα** του υπευθύνου επεξεργασίας ή τρίτων

Σύννομη επεξεργασία των δεδομένων υγείας (1/2)

- Η επεξεργασία δεδομένων υγείας ***καταρχήν απαγορεύεται.***
- **ΕΠΙΤΡΕΠΟΜΕΝΕΣ ΕΞΑΙΡΕΣΕΙΣ:**
  - Όταν υπάρχει **συγκατάθεση μετά από ενημέρωση («informed consent»)** του υποκειμένου
  - Εκπλήρωση υποχρεώσεων/άσκηση δικαιωμάτων του Υπευθύνου Επεξεργασίας ή του υποκειμένου σχετικά με την κοινωνική ασφάλιση/κοινωνική προστασία
  - **Προστασία ζωτικών συμφερόντων του** υποκειμένου των δεδομένων ή άλλου προσώπου, όταν το υποκείμενο είναι **σωματικά ή νομικά* ανίκανο να συγκατατεθεί.**

Σύννομη επεξεργασία των δεδομένων υγείας (1/2)

- Ουσιαστικό δημόσιο συμφέρον στον τομέα της υγείας (π.χ. προστασία έναντι διασυνοριακών απειλών κατά της υγείας, διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας υγειονομικών υπηρεσιών και προϊόντων)
- Προληπτική ή επαγγελματική ιατρική
- Εκτίμηση της ικανότητας προς εργασία
- Ιατρική διάγνωση/θεραπεία
- Παροχή υγειονομικής ή κοινωνικής περίθαλψης
- Διαχείριση υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών
- Δυνάμει σύμβασης με επαγγελματία υγείας που υπόκειται στην υποχρέωση τήρησης του ιατρικού απορρήτου
- Επιστημονική/ιστορική έρευνα

Προϋποθέσεις συγκατάθεσης (1/2)

- Ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να αποδείξει την ύπαρξη συγκατάθεσης
- Το αίτημα **υποβάλλεται κατά τρόπο ώστε** να είναι
  - σαφώς διακριτό από άλλα θέματα,
  - σε κατανοητή και εύκολα προσβάσιμη μορφή,
  - με σαφή και απλή διατύπωση.
- **Δικαίωμα ανάκλησης** συγκατάθεσης
  - Εξίσου εύκολη με την παροχή της

Προϋποθέσεις συγκατάθεσης (2/2)

- **Απαιτείται πράγματι η συγκατάθεση του υποκειμένου** για τις ανάγκες εκτέλεσης μιας σύμβασης ή παροχής υπηρεσίας;
  - Ο υπεύθυνος επεξεργασίας δε θα πρέπει να υπερβαίνει τα απαραίτητα

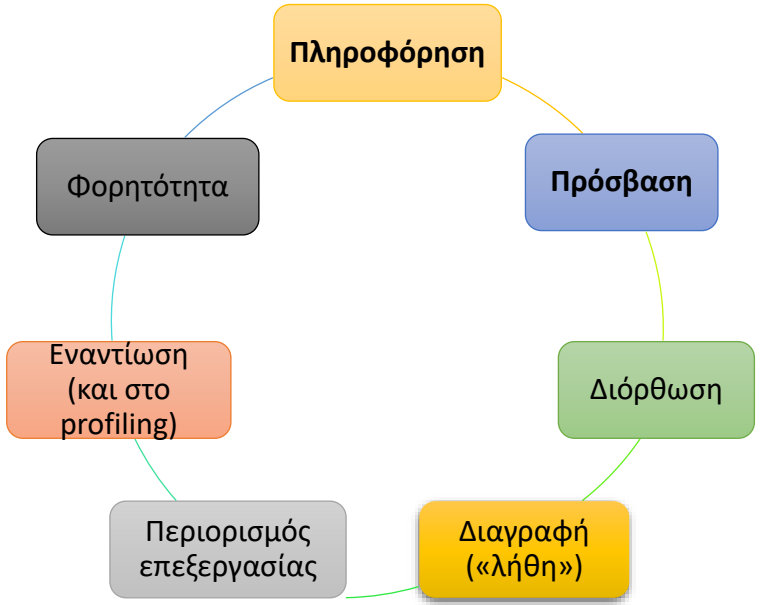
Ειδικότερα η συγκατάθεση του ασθενούς

- Ο GDPR προέβλεψε τη **σωματική και τη νομική ανικανότητα του υποκειμένου να συγκατατεθεί** στην επεξεργασία των δεδομένων του
- Η **σωματική ανικανότητα** του υποκειμένου αποτελεί **αντικείμενο εκτίμησης/αξιολόγησης της ψυχικής/νοητικής/σωματικής κατάστασης του ασθενούς από τον Υπεύθυνο Επεξεργασίας με τη συνδρομή ειδικού θεράποντος ιατρού**
- Εν τέλει η εκτίμηση της «σωματικής ανικανότητας» από τον Υπεύθυνο Επεξεργασίας θα αξιολογηθεί και από την Εποπτική Αρχή κατά τον έλεγχο της συμμόρφωσης
- Η **νομική ανικανότητα** ανάγεται στο εθνικό δίκαιο των κρατών μελών. Στο ελληνικό δίκαιο η νομική ανικανότητα ταυτίζεται με την «ανικανότητα προς δικαιοπραξία»

Επεξεργασία δεδομένων σε περίπτωση ανικανότητας συγκατάθεσης

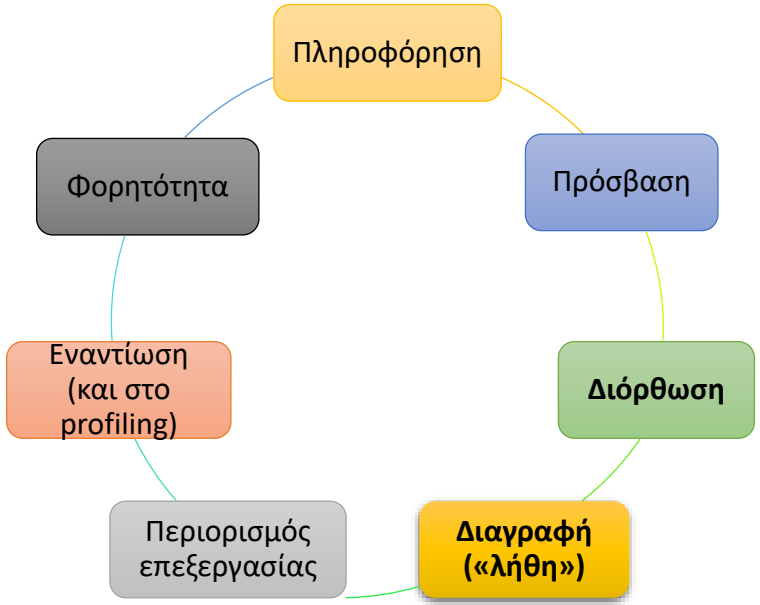
Δικαιώματα υποκειμένου (1/3)

- Δικαίωμα **στην πληροφόρηση**
  - Είτε τα δεδομένα συλλέγονται από το υποκείμενο είτε από άλλες πηγές
  - Παρέχεται με εύκολο τρόπο, απλή και κατανοητή γλώσσα, και δωρεάν
  - Περιλαμβάνει σκοπούς επεξεργασίας, νομική βάση, πιθανούς αποδέκτες, διάστημα επεξεργασίας, δικαιώματα υποκειμένου
- Δικαίωμα **στην πρόσβαση**
  - Σε αντίγραφο των δεδομένων και σε όλες τις πληροφορίες που αφορούν στην επεξεργασία



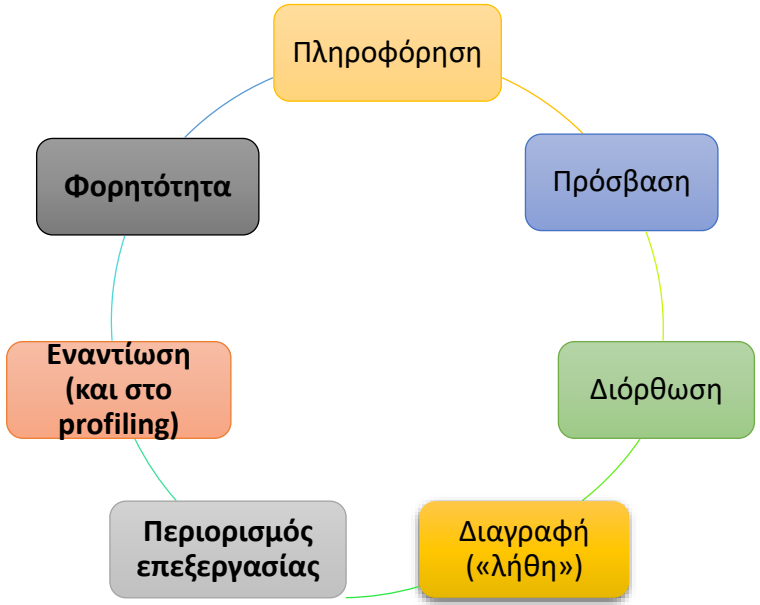
Δικαιώματα υποκειμένου (2/3)

- Δικαίωμα **διόρθωσης**
  - Ανακριβείς ή ελλιπείς πληροφορίες θα πρέπει να διορθωθούν
  - Αν τα δεδομένα έχουν δοθεί σε τρίτους θα πρέπει να επικαιροποιηθούν και αυτά
- Δικαίωμα **διαγραφής (στη λήθη)**
  - Όταν τα δεδομένα δεν απαιτούνται για τον αρχικό τους σκοπό, το υποκείμενο ανακαλεί τη συγκατάθεση του, ή αντιτίθεται στην επεξεργασία
  - Δεν είναι εφικτή εάν υπάρχουν νομικές υποχρεώσεις ή δημόσιο συμφέρον



Δικαιώματα υποκειμένου (3/3)

- Δικαίωμα **περιορισμού της επεξεργασίας**
  - Αμφισβητείται η ακρίβεια των δεδομένων
  - Κοινοποίηση του περιορισμού σε τρίτους που επεξεργάζονται τα δεδομένα
- Δικαίωμα **εναντίωσης**
  - Στην επεξεργασία, συμπεριλαμβανομένης της αυτοματοποιημένης λήψης αποφάσεων, της δημιουργίας προφίλ, και για διαφημιστικούς σκοπούς
- Δικαίωμα **στη φορητότητα**
  - Σε άλλον υπεύθυνο επεξεργασίας, χωρίς καμία αντίρρηση και με τη χρήση κοινά χρησιμοποιούμενων μορφότυπων, π.χ. CSV αρχεία



Υπεύθυνος επεξεργασίας (1/2)

(Data controller)

- **Φυσικό** ή **νομικό πρόσωπο**, **δημόσια αρχή**, **υπηρεσία** ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους **σκοπούς και τον τρόπο της επεξεργασίας** δεδομένων προσωπικού χαρακτήρα

- Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους

Υπεύθυνος επεξεργασίας (2/2)

(Data controller)

- Εφαρμόζει κατάλληλα **τεχνικά και οργανωτικά μέτρα** για να διασφαλίζει ότι, **εξ ορισμού**, υφίστανται επεξεργασία μόνο στα δεδομένα προσωπικού χαρακτήρα που είναι **απαραίτητα** για τον εκάστοτε σκοπό της επεξεργασίας
- **Γνωστοποίηση** παραβιάσεων δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή **μέσα σε 72 ώρες** από τη στιγμή που αποκτά γνώση του γεγονότος

Ο εκτελών την επεξεργασία (1/2)

(Data processor)

- Θα πρέπει να παρέχει επαρκείς **διαβεβαιώσεις** από πλευράς **εμπειρογνωμοσύνης**, **αξιοπιστίας** και **πόρων** για την ασφάλεια της επεξεργασίας
- Η επεξεργασία **γίνεται βάσει σύμβασης** που καθορίζει
  - αντικείμενο και διάρκεια επεξεργασίας,
  - φύση και σκοποί επεξεργασίας,
  - είδος δεδομένων προσωπικού χαρακτήρα και
  - κατηγορίες υποκειμένων δεδομένων

Ο εκτελών την επεξεργασία (2/2)

(Data processor)

- Με το πέρας της επεξεργασίας
  - Τα προσωπικά δεδομένα επιστρέφονται ή διαγράφονται εκτός αν υπάρχουν άλλες νομικές δεσμεύσεις

- Σημαντικός ο **έλεγχος** και, όπου απαιτείται, η **αναθεώρηση των συμβάσεων**

3| Health Insurance Portability and Accountability Act (HIPAA)

What laws in the US protect health records?

Maintaining privacy of health records is governed by many laws and regulations:

1. HIPAA
2. The HITECH Act
3. 42 C.F.R. Part 2-Substance Abuse Records
4. Federal Privacy Act (5 USC § 552a (b))
5. State law

HIPAA

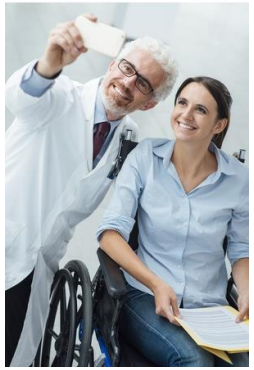
- HIPAA is an acronym that stands for the Health Insurance Portability and Accountability Act of 1996
- HIPAA applies to Doctors, employees of health care organizations, students, volunteers, contractors and vendors
- HIPAA Penalties:
  - HIPAA Civil Penalties
    - $100 - $25,000 / year fines; More fines if multiple year violations
  - HIPAA Criminal Penalties
    - $50,000 - $1,500,000 fines; Imprisonment up to 10 years
  - State Laws
    - Fines and penalties apply to individuals as well as health care providers, up to a maximum of $250,000; may impact your professional license
    - Imprisonment up to 10 years

HIPAA governs Protected Health Information (PHI)

- PHI is a subset of health information that is:
  - created or received by a health care provider
  - related to the past, present, or future health of an individual
  - related to the past, present or future payment for the provision of health care to an individual
  - **Identifying information**
  - Demographic information

What is “Identifying Information”?

- Name
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Any vehicle or other device serial number
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image – note images are not limited to images of the face
- **Any other characteristic that could uniquely identify the individual**



HIPAA is broken into 3 Rules

- Privacy
- Security
- Breach Notification

HIPAA Rule #1: Privacy Rule

- Establishes national standards to protect individuals' medical records and other PHI
- Requires appropriate safeguards to protect the privacy of PHI, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization
- The Rule also gives **patients rights** over their health information, including rights to examine and obtain a copy of their health records, and to request corrections

How do patients know their rights?

Healthcare facilities must have a Notice of Privacy Practices (NPP)

- Each patient should receive a copy of the NPP at the time that they first receive treatment and again whenever the NPP is substantively changed
- The NPP should be posted in patient areas and on your website

Permitted Use and Disclosure of PHI

- PHI may be used and disclosed to facilitate TPO, which means:
  - For **T**reatment
  - For **P**ayment
  - For certain healthcare **O**perations, such as quality improvement, credentialing, compliance, and patient/employee safety activities

Authorizations and Patient's Right to Access their PHI

- A covered entity may generally use and disclose PHI to a third party if it gets the patient's signed HIPAA-valid authorization
  - However, a HIPAA authorization form should not be used when a patient asks for a copy of their PHI for themselves or to be sent to a third party – in that case, use a Patient Request for Health Information Form
  - It is a HIPAA violation to use the wrong form in this circumstance (the regulations require different information on each form)
  - The fees that can be charged for a copy of a patient's PHI or record differs based on whether the records are being released per an Authorization or a Patient's Request
  - A covered entity can only charge a reasonable, cost-based amount when a patient requests the records – It is permissible to charge up to $6.50 for a flat fee for electronic copies (for labor, supplies and postage)

Minimum Necessary Standard

- When HIPAA permits use or disclosure of PHI, a covered entity must use or disclose only the **minimum necessary** PHI required to accomplish the purpose of the use or disclosure.
- The only exceptions to the minimum necessary standard are those times when a covered entity is disclosing PHI for the following reasons:
  - Treatment
  - Purposes for which an authorization is signed
  - Disclosures required by law
  - Sharing information to the patient about himself/herself

HIPAA Rule #2: Security Rule

- The Security Rule establishes national standards to protect individuals' electronic PHI (e-PHI) that is created, received, used, or maintained by a covered entity
  - HIPAA security standards ensure the confidentiality, integrity, and availability of PHI
- The Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of e-PHI
  - Protect against any reasonably anticipated threats or hazards to the security or integrity or such information
  - Protect against any reasonably anticipated uses or disclosures of such information that are not permitted

Rules for Access

- Access to computer systems and information is based on your work duties and responsibilities
- Access privileges are limited to only the minimum necessary information you need to do your work
- Access to an information system does not automatically mean that you are authorized to view or use all the data in that system
- Different levels of access for personnel to PHI is intentional
- If job duties change, clearance levels for access to PHI is re-evaluated
- Access is eliminated if employee is terminated
- Accessing PHI for which you are not cleared or for which there is no job-related purpose will subject you to sanctions

Rules for Protecting Information

- Do not allow unauthorized persons into restricted areas where access to PHI could occur
- Arrange computer screens so they are not visible to unauthorized persons and/or patients; use security screens in areas accessible to public
- Log in with password, log off prior to leaving work area, and do not leave computer unattended
- Close files not in use/turn over paperwork containing PHI
- Do not duplicate, transmit, or store PHI without appropriate authorization
- Storage of PHI on unencrypted removable devices (Disk/CD/DVD/Flash Drives) is prohibited without prior authorization

HIPAA Rule #3: Breach Notification Rule

- The Breach Notification Rule requires **covered entities** and their business associates to provide notification following a breach of unsecured PHI
- The covered entity must notify the affected individual **without unreasonable delay**, but not later than **60 calendar days** from discovering the breach
  - Time runs when incident first known or reasonably should have been known (true for covered entity and business associate), NOT when it is determined that a breach occurred
  - Breach is treated as discovered when workforce member or other agent has knowledge of incident
  - Delay permissible in certain circumstances where law enforcement has requested a delay

What Constitutes a Breach?

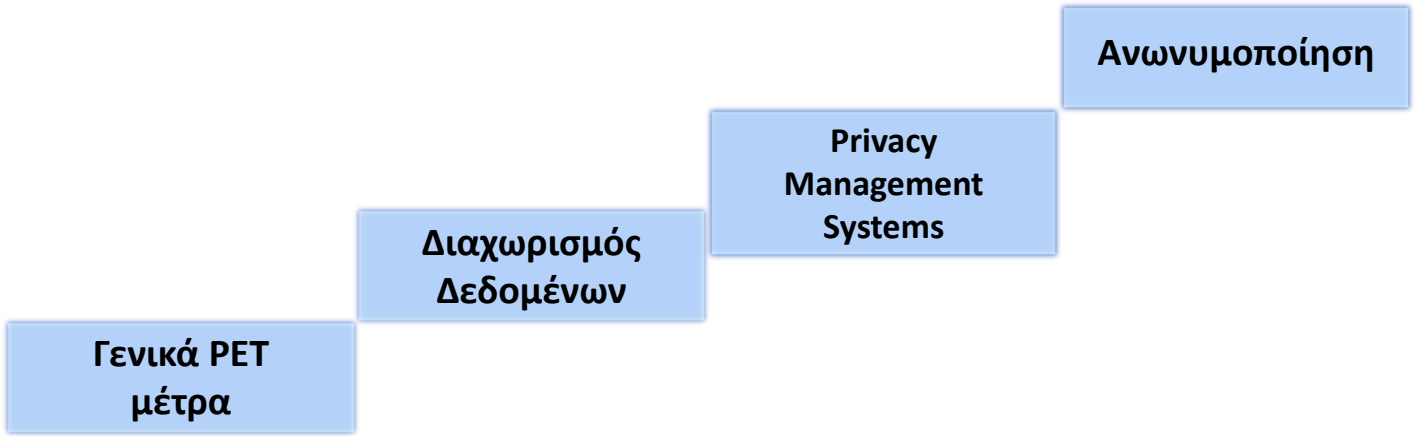
- A breach could result from many activities:
  - Accessing more than the minimum necessary
  - Failing to log off when leaving a workstation
  - Unauthorized access to PHI
  - Sharing confidential information, including passwords
  - Having patient-related conversations in public settings
  - Improper disposal of confidential materials in any form
  - Copying or removing PHI from the appropriate area

- Why?
  - Curiosity…about a co-worker or friend
  - Laziness…so shared sign-on to information systems
  - Compassion…the desire to help someone
  - Greed or malicious intent…for personal gain

4| Ενδεικτικά μέτρα συμμόρφωσης με το GDPR και HIPAA

Πρόκληση

- Εφαρμογή κατάλληλων **Privacy Enhancing Technologies**
- Συμπληρώνουν τα όποια μέτρα ασφαλείας



Μέτρα που θα πρέπει να λάβουμε υπόψη

- Ανωνυμοποίηση
  - Για δεδομένα όπου δεν απαιτείται ταυτοποίηση
- Ψευδωνυμοποίηση

Κρυπτογράφηση (1/3)

- Επιλογή κατάλληλων αλγορίθμων (τυποποιημένων) και κλειδιών βάσει των απαιτήσεων των δεδομένων και του συστήματος αρχειοθέτησης
- Λήψη μέτρων ώστε να εξασφαλιστεί η διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των κλειδιών
- Κρυπτογράφηση δίσκων σε επίπεδο υλικού (όλο τον δίσκο) ή σε επίπεδο ΛΣ (partitions)
  - Χρήση μέσων αποθήκευσης με τεχνολογία SED (self-encrypting drives)
  - Χρήση λογισμικού όπως dm-crypt (Linux), FileVault (MacOS), και VeraCrypt (Windows)

Κρυπτογράφηση (2/3)

- Βάσεων δεδομένων:
  - Σε επίπεδο υλικού, λειτουργικού συστήματος, βάσης δεδομένων, εφαρμογής που διαχειρίζεται τα δεδομένα της βάσης
- Αρχείων
  - ZoneCentral (CC EAL3+), AxCrypt , Gnu Privacy Guard (GPG)

Κρυπτογράφηση (3/3)

- Emails
  - Gnu Privacy Guard (GPG)
- Επικοινωνίες
  - TLS, SSH, IPSec (VPNs)
- Μπορεί να απαιτείται η χρήση κάποιου hardware security module (HSM)

Hardware-based encryption

- Crypto accelerators
  - PCI card
  - NetHSM
  - USB

TAMPER RESISTANT

- Smart cards

Μέτρα που θα πρέπει να λάβουμε υπόψη (1/5)

- Διατήρηση της ακεραιότητας
  - Hash, MAC, υπογραφές
  - Χρήση έξυπνων καρτών
  - blockchain
- Διαχωρισμός ρόλων (segregation of duties)
- Διαχωρισμός δεδομένων (από τα υπόλοιπα)

Μέτρα που θα πρέπει να λάβουμε υπόψη (2/5)

- Φυσικός έλεγχος πρόσβασης
- Λογικός έλεγχος πρόσβασης
  - need-to-know principle
  - Authentication
  - Διαχείριση διαπιστευτηρίων
- Περιορισμό της διάρκειας αποθήκευσης των δεδομένων – όχι περισσότερο απ’όσο χρειάζονται

Μέτρα που θα πρέπει να λάβουμε υπόψη (3/5)

- Αποφυγή ενεργειών υψηλού ρίσκου
  - εγκατάσταση σε επικίνδυνες γεωγραφικές περιοχές
  - μετάδοση δεδομένων σε τρίτες χώρες
- Προσδιορισμός των σκοπών επεξεργασίας και της νομικής βάσης

Μέτρα που θα πρέπει να λάβουμε υπόψη (4/5)

- Προετοιμασία για την εξυπηρέτηση των δικαιωμάτων των υποκειμένων
  - μέσω εναλλακτικών καναλιών: τηλεφώνου, email, ηλεκτρονικής φόρμας
- Διαχείριση συμβάντων και περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα

Μέτρα που θα πρέπει να λάβουμε υπόψη (5/5)

- Διαχείριση σταθμών εργασίας και συσκευών
  - Mobile devices, smartphones
- Διαχείριση έργων
  - Απαιτήσεις για του υπεργολάβους
  - Μέτρα για την προμήθεια εξοπλισμού αλλά και την προμήθεια/ανάπτυξη λογισμικού

σε αυτό το μάθημα είδαμε…

- Ποιες είναι οι διαφορές του GDPR και του HIPAA
- Τι περιλαμβάνει ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) στην Ευρώπη
- Τι περιλαμβάνει ο νόμος HIPAA στις Ηνωμένες Πολιτείες
- Κάποια ενδεικτικά μέτρα συμμόρφωσης με το GDPR και HIPAA

ΕΥΧΑΡΙΣΤΩ/**GRÀCIES**/HVALA/DĚKUJI/TAK/**DANK**
JEWEL/AITÄH/KIITOS/MERCI/**DANKE**/KÖSZNÖNÖ/
GRAZIE/PALDIES/**AČIŪ**/GRAZZI/TAKK/DZIĘKUJĘ
OBRIGADO/MULTUMESC/**СПАСИБО**/ХВАЛА
HVALA/**БЛАГОДАРЯ**/THANKYOU/TAK/GRACIAS
/**KIITOS**/TACK/TEŞEKKÜREDERİM/**СПАСИБІ**/
JUFALEMINDERIT/**ΕΥΧΑΡΙΣΤΩ**/DANKJEWEL/TAK
TACK/**GRAZZI**/DANKJEWEL/MULTUMESC/AITÄH
KÖSZNÖNÖ/СПАСИБО/**ХВАЛА**/AČIŪ/**THANKYOU**

Ύλη μαθήματος

- Διαφάνειες μαθήματος
- European Parliament and Council, “Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),” Official Journal of the European Union, 2016. http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679
- 104th US Congress, Public Law 104 - 191 - Health Insurance Portability and Accountability Act of 1996, Public and Private Laws, 1996. https://www.govinfo.gov/app/details/PLAW-104publ191

Για αναφορά στις διαφάνειες χρησιμοποιείστε το παρακάτω:

Γ. Δροσάτος, Διαλέξεις Μεταπτυχιακού Μαθήματος “Πιστοποίηση Ποιότητας και Αξιολόγηση Τεχνολογιών Υγείας”, ΠΜΣ Έρευνα και Καινοτομία στις Επιστήμες Υγείας, Τμήμα Ιατρικής, Δημοκρίτειο Πανεπιστήμιο Θράκης, 2024 (https://rih.med.duth.gr)

Cite this presentation as:

G. Drosatos, Postgraduate Lectures in “Health Technology Quality Assurance and Assessment”, MSc in Research and Innovation in Health Sciences, School of Medicine, Democritus University of Thrace, Greece, 2024 (https://rih.med.duth.gr)