

Δραστηριότητα: Διαχείριση δεδομένων στην πράξη

Στόχος:

Οι συμμετέχοντες θα εφαρμόσουν τις γνώσεις τους σχετικά με τη διαχείριση δεδομένων περιγράφοντας τα βήματα για τη διαχείριση, αποθήκευση και προστασία δεδομένων σε ένα πραγματικό σενάριο. Θα επικεντρωθούν στην επιλογή των πηγών δεδομένων, στην αποτελεσματική οργάνωση των δεδομένων και στη διασφάλιση της συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων.

Διάρκεια:

30 λεπτά

Απαιτούμενα υλικά:

- Φυλλάδια ή ψηφιακά αρχεία με την περιγραφή του σεναρίου.
 - Χαρτί ή ψηφιακές συσκευές για να περιγράψουν οι συμμετέχοντες τα βήματά τους.
 - Ένα χρονόμετρο.
-

Οδηγίες:

1. Εισαγωγή (5 λεπτά):

Εξηγήστε εν συντομία τους στόχους της άσκησης:

- Οι συμμετέχοντες θα ενεργήσουν ως επαγγελματίες διαχείρισης δεδομένων που πρέπει να σχεδιάσουν μια στρατηγική διαχείρισης δεδομένων για ένα δεδομένο σενάριο.
 - Τονίστε ότι θα πρέπει να εξετάσουν τις πηγές δεδομένων, τις επιλογές αποθήκευσης, την οργάνωση και την προστασία των δεδομένων (συμπεριλαμβανομένης της συμμόρφωσης με τον GDPR).
-

2. Σενάριο (15 λεπτά):

Δώστε στους συμμετέχοντες το ακόλουθο σενάριο για να δουλέψουν:

Σενάριο:

Εργάζεστε ως σύμβουλος διαχείρισης δεδομένων για έναν οργανισμό υγειονομικής περίθαλψης που μεταβαίνει από τα έντυπα αρχεία σε ένα πλήρως ψηφιακό σύστημα. Ο οργανισμός ασχολείται με ευαίσθητα δεδομένα ασθενών, συμπεριλαμβανομένων ιατρικών αρχείων, προγραμμάτων ραντεβού και πληροφοριών τιμολόγησης.



Εργασία:

Περιγράψτε τα μέτρα που θα λαμβάνετε για τη διαχείριση, την αποθήκευση και την προστασία αυτών των δεδομένων. Το σχέδιό σας θα πρέπει να καλύπτει τα εξής:

- **Πηγές δεδομένων:**
 - Προσδιορίστε και κατηγοριοποιήστε τις πηγές δεδομένων (π.χ. αρχεία ασθενών, εργαστηριακά αποτελέσματα, πληροφορίες τιμολόγησης).
- **Αποθήκευση δεδομένων:**
 - Προτείνετε την καλύτερη μέθοδο αποθήκευσης για τα δεδομένα (αποθήκευση σε νέφος ή φυσικούς διακομιστές) και εξηγήστε τους λόγους.
 - Εξετάστε την επεκτασιμότητα, την προσβασιμότητα και τη σχέση κόστους-αποτελεσματικότητας.
- **Οργάνωση δεδομένων:**
 - Προτείνετε ένα σύστημα για την οργάνωση των δεδομένων (δομημένα ή μη δομημένα) και προτείνετε εργαλεία ή πλατφόρμες (π.χ. DBMS, πλατφόρμες cloud).
 - Εξηγήστε πώς θα μπορούσαν να χρησιμοποιηθούν μεταδεδομένα για να διασφαλιστεί ότι τα δεδομένα είναι εύκολα ανακτήσιμα.
- **Προστασία δεδομένων:**
 - Περιγράψτε τον τρόπο με τον οποίο θα διασφαλίσετε την ασφάλεια των δεδομένων και τη συμμόρφωση με τον ΓΚΠΔ.
 - Συμπεριλάβετε μεθόδους κρυπτογράφησης, μέτρα ελέγχου πρόσβασης και πρακτικές προστασίας του απορρήτου των δεδομένων.

3. Ατομική εργασία (10 λεπτά):

- Οι συμμετέχοντες θα εργαστούν ατομικά για να δημιουργήσουν ένα δομημένο σχέδιο για τη διαχείριση, αποθήκευση και προστασία των δεδομένων στο συγκεκριμένο σενάριο.
- Ενθαρρύνετέ τους να σκεφτούν κριτικά για τα πλεονεκτήματα και τα μειονεκτήματα των διαφορετικών μεθόδων αποθήκευσης, των εργαλείων οργάνωσης και των μέτρων ασφαλείας.

4. Παρουσίαση και ανατροφοδότηση (10 λεπτά):

- Κάθε συμμετέχων θα παρουσιάσει το σχέδιό του στην ομάδα, εξηγώντας τις επιλογές του για τη διαχείριση, την αποθήκευση και την προστασία των δεδομένων.



- Ο διαμεσολαβητής θα παρέχει ανατροφοδότηση, επισημαίνοντας τα δυνατά σημεία και τους τομείς που χρήζουν βελτίωσης, ιδίως όσον αφορά την ασφάλεια των δεδομένων και τη συμμόρφωση με τον ΓΚΠΔ.

Βασικά μαθησιακά αποτελέσματα:

- Οι συμμετέχοντες θα μάθουν πώς να σχεδιάζουν μια στρατηγική διαχείρισης δεδομένων για ένα πραγματικό σενάριο.
- Θα αναπτύξουν δεξιότητες κριτικής σκέψης σχετικά με τις επιλογές αποθήκευσης δεδομένων και τα μέτρα ασφαλείας.
- Θα κατανοήσουν πώς να διασφαλίζουν τη συμμόρφωση με τους νόμους περί προστασίας δεδομένων, όπως ο GDPR.

Παράδειγμα Task Response: Σχέδιο διαχείρισης δεδομένων για έναν οργανισμό υγειονομικής περίθαλψης

Πηγές δεδομένων:

- **Αρχεία ασθενών:**
 - Περιλαμβάνει ιατρικό ιστορικό, εργαστηριακά αποτελέσματα, διαγνώσεις και σχέδια θεραπειών. Συλλέγεται από γιατρούς, νοσηλευτές και τεχνικούς εργαστηρίων.



- **Προγράμματα ραντεβού:**
 - Δεδομένα σχετικά με τα ραντεβού των ασθενών, συμπεριλαμβανομένης της ημερομηνίας, της ώρας και του τύπου της υπηρεσίας (π.χ. διαβουλεύσεις, χειρουργεία).
- **Πληροφορίες χρέωσης:**
 - Δεδομένα σχετικά με τις ασφαλιστικές απαιτήσεις, τις πληρωμές και τα ανεξόφλητα υπόλοιπα των ασθενών.

Αποθήκευση δεδομένων:

- **Σύσταση:**
 - Χρησιμοποιήστε **αποθήκευση στο νέφος** για επεκτασιμότητα, οικονομική αποδοτικότητα και εύκολη πρόσβαση από πολλές τοποθεσίες (σημαντικό για την τηλεϊατρική και την απομακρυσμένη πρόσβαση).
 - **Γιατί αποθήκευση στο Cloud;**
 - Επιτρέπει την αυτόματη δημιουργία αντιγράφων ασφαλείας, μειώνοντας τον κίνδυνο απώλειας δεδομένων.
 - Παρέχει υψηλή προσβασιμότητα για το ιατρικό προσωπικό από οποιαδήποτε θέση, βελτιώνοντας τη συνεργασία.
 - Ευέλικτες επιλογές αποθήκευσης που αναπτύσσονται με τις ανάγκες του οργανισμού.
- **Επιλογές παρόχων cloud:**
 - Το **Google Cloud Healthcare API** ή το **Amazon Web Services (AWS)** μπορούν να παρέχουν αποθήκευση στο cloud σύμφωνα με το HIPAA για ευαίσθητα δεδομένα υγειονομικής περίθαλψης.

Οργάνωση δεδομένων:

- **Δομημένα δεδομένα:**
 - Τα ιατρικά αρχεία, οι πληροφορίες χρέωσης και τα χρονοδιαγράμματα ραντεβού θα αποθηκεύονται σε δομημένη μορφή χρησιμοποιώντας ένα **σύστημα διαχείρισης βάσεων δεδομένων (DBMS)** (π.χ. **PostgreSQL, MySQL**).
 - Χρησιμοποιήστε μεταδεδομένα (π.χ. ταυτότητα ασθενούς, ημερομηνία ραντεβού) για να καταστήσετε τα δεδομένα εύκολα αναζητήσιμα και ανακτήσιμα.
- **Μη δομημένα δεδομένα:**



- Οποιοσδήποτε ιατρικές εικόνες ή σαρώσεις (π.χ. ακτινογραφίες, μαγνητικές τομογραφίες) θα αποθηκεύονται στο σύννεφο ως μη δομημένα δεδομένα, χρησιμοποιώντας εργαλεία όπως το **Google Cloud Storage** με κατάλληλες ετικέτες μεταδεδομένων για κατηγοριοποίηση.
- **Εργαλεία που χρησιμοποιήθηκαν:**
 - **DBMS** για τη διαχείριση δομημένων δεδομένων ασθενών και τιμολόγησης.
 - **Διαχείριση αρχείων** ιατρικών εικόνων και εγγράφων **με βάση το cloud**.

Προστασία και ασφάλεια δεδομένων:

- **Συμμόρφωση GDPR:**
 - Διασφαλίστε ότι οι ασθενείς παρέχουν τη συγκατάθεσή τους για τη συλλογή και την ψηφιακή αποθήκευση των δεδομένων τους.
 - Εφαρμόστε ένα σύστημα όπου οι ασθενείς έχουν το δικαίωμα να ζητούν πρόσβαση στα δεδομένα τους και να ζητούν τη διαγραφή τους όταν είναι απαραίτητο.
- **Κρυπτογράφηση:**
 - Χρησιμοποιήστε **κρυπτογράφηση από άκρο σε άκρο** για την προστασία των δεδομένων κατά τη διαμετακόμιση μεταξύ του ιατρικού προσωπικού και των διακομιστών νέφους. Κρυπτογραφήστε τα αρχεία ασθενών και τα δεδομένα χρέωσης, διασφαλίζοντας ότι ακόμη και αν τα δεδομένα υποκλαπούν, δεν μπορούν να διαβαστούν.
- **Έλεγχος πρόσβασης:**
 - Εφαρμογή **ελέγχου πρόσβασης βάσει ρόλων (RBAC)** για τον περιορισμό της πρόσβασης σε ευαίσθητα δεδομένα. Για παράδειγμα:
 - Μόνο οι γιατροί και το εξουσιοδοτημένο ιατρικό προσωπικό μπορούν να έχουν πρόσβαση στα ιατρικά αρχεία των ασθενών.
 - Το διοικητικό προσωπικό μπορεί να έχει πρόσβαση στα προγράμματα ραντεβού και στις πληροφορίες χρέωσης, αλλά όχι στα ιατρικά αρχεία.
- **Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA):**
 - Απαιτήστε από όλους τους χρήστες (π.χ. γιατρούς, νοσηλευτές, διοικητικό προσωπικό) να χρησιμοποιούν MFA κατά την πρόσβαση στο σύστημα, ώστε να διασφαλίζεται ότι μόνο εξουσιοδοτημένο προσωπικό μπορεί να βλέπει ευαίσθητα δεδομένα ασθενών.
- **Τακτικοί έλεγχοι και παρακολούθηση:**
 - Εφαρμόστε τακτικούς ελέγχους ασφαλείας και παρακολούθηση των αρχείων καταγραφής πρόσβασης για τον εντοπισμό τυχόν μη εξουσιοδοτημένων προσπαθειών πρόσβασης ή ύποπτων δραστηριοτήτων.



Περίληψη του σχεδίου:

- Οι πηγές δεδομένων έχουν εντοπιστεί και κατηγοριοποιηθεί (αρχεία ασθενών, ραντεβού, τιμολόγηση).
- Η αποθήκευση στο νέφος επιλέγεται για την επεκτασιμότητα και την προσβασιμότητά της, με μέτρα ασφαλείας (κρυπτογράφηση, έλεγχος πρόσβασης).
- Τα δεδομένα θα οργανωθούν με τη χρήση ενός DBMS για δομημένα δεδομένα και με αποθήκευση στο νέφος για μη δομημένα δεδομένα.
- Η στρατηγική διαχείρισης δεδομένων διασφαλίζει τη συμμόρφωση με τον GDPR, την κρυπτογράφηση και τον αυστηρό έλεγχο πρόσβασης.

