Piattaforma Incepto Folio e Tango-Sistemi

TO TRANSLATE - Evaluation :
SCUDO PRYVACY
TO TRANSLATE - Validation :
ALIQUO' ANGELO
TO TRANSLATE - Status :
In corso
60%

TO TRANSLATE - Validation

Mappaggio dei rischi

TO TRANSLATE - Validation

Piano d'azione

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

TO TRANSLATE - Validation

TO TRANSLATE - DPO and data subjects opinion

TO TRANSLATE - No data to display.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Aggregazione di diverse soluzioni di IA in radiologia.

Integrazione nella routine clinica.

Installazione su una macchina virtuale all'interno della rete dell'istituto.

Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento: AO San Camillo Forlanini

Responsabile: Società INCEPTO Italia

Soggetto Designato per le finalità di tutela del patrimonio:
Direttore UOC Economato e Gestione Contratti
Cura: Direttore Sanitario

Ci sono standard applicabili al trattamento?

- rispetto del GDPR (UE 2016/679);
  adozione di standard di sicurezza delle informazioni (es. ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701);
  applicazione delle linee guida del Garante per la protezione dei dati personali e dell'EDPB;
  Implementazione di best practice in materia di gestione documentale, controllo accessi, logging e conservazione dei dati

Contesto

Dati, processi, risorse di supporto e categoria di dati interessati

Quali sono i dati trattati?

Nome, cognome, data di nascita e sesso dei pazienti.
Nome e cognome dei dipendenti della Azienda Ospedaliera.
ID paziente/ numero della cartella clinica
Dati relativi alla salute e immagini di refertazione.
Nome reparto e unità operativa

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il ciclo di vita dei dati trattati mediante la piattaforma INCEPTO Folio si articola nelle seguenti fasi: raccolta e inserimento dei dati, classificazione e registrazione, archiviazione e conservazione attiva, utilizzo e consultazione nell'ambito dei processi aziendali, eventuale condivisione.

I dati sono conservati nei sistemi clinici aziendali secondo le regole di conservazione della documentazione sanitaria e possono essere

successivamente utilizzati, in forma aggregata o pseudonimizzata, per finalità di audit clinico, controllo di qualità o attività di ricerca nel rispetto della normativa applicabile.

Quali sono le risorse di supporto ai dati?

Gli apparati dedicati alla gestione del servizio sono i seguenti:
La piattaforma incepto Folio e Incepto Tango (applicativo)

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Specifici: è ben delineata ed individuata nella necessità del titolare del trattamento di svolgere attività di utilizzo di soluzioni di IA in radiologia e Integrazione nella routine clinica.

Espliciti in quanto esplicitati nelle informazioni privacy ex art. 13 GDPR somministrate agli interessati

Legittimi: in quanto sorretta da un'idonea base giuridica, rappresentata dall'art. 6, par. 1, lett. e), dall'art. 9, par. 2, lett. h) GDPR.

Quali sono le basi legali che rendono lecito il trattamento?

Art. 6, par. 1, lett. e)

Art. 9, par. 2, lett. h) GDPR

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Sono trattati esclusivamente i dati necessari al perseguimento della finalità di cura del paziente.

Pertanto, i dati raccolti risultano adeguati, pertinenti e limitati rispetto alla specifica finalità.

I dati sono esatti e aggiornati?

Per loro natura i dati in oggetto sono esatti ed aggiornati

Qual è il periodo di conservazione dei dati?

La durata della conservazione dei dati è tre giorni (tempo necessario di indagine necessario in caso di fallimento del trattamento), previsto dalla lifecycle policy di AWS S3

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Con le informazioni privacy ex art. 13 GDPR

Ove applicabile: come si ottiene il consenso degli interessati?

N.A.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Tramite formale richiesta al titolare via mail

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Tramite formale richiesta al titolare via mail

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Tramite formale richiesta al titolare via mail

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

SI

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

N.A.

Rischi

Misure esistenti o pianificate

Crittografia

Tutti i dati in transito sono crittografati utilizzando il protocollo HTTPS (TLS 1.2 o superiore). A riposo, i dati identificativi dei pazienti (criptati dal Gateway prima del trasferimento per scopi di identitovigilanza) sono archiviati all'interno di un database dedicato e crittografato (encrypted-at-rest)

Anonimizzazione

N.A.

Pseudonimizzazione

Le immagini DICOM vengono fortemente pseudonimizzate dal Gateway locale prima di essere inviate al Cloud, in conformità con la norma ISO 25237 e lo standard DICOM PS3.15 allegato E. Tutti i dati di identificazione diretta (nome, ID paziente, ecc.) e la maggior parte di quelli indiretti vengono rimossi o modificati, ad eccezione delle date. Inoltre, le immagini che potrebbero avere informazioni sanitarie "bruciate" nei pixel (Secondary Captures) vengono ignorate di default o oscurate (tramite black box). Nessuna informazione identificativa viene conservata nel Pixel Data

Partizionamento

I dati sono strettamente segregati e partizionati in tre database distinti: un database temporaneo sul Gateway locale, un database (completamente crittografato) per i soli identificativi dei pazienti e un database finale per le immagini pseudonimizzate

. Un token utente contiene i diritti di accesso specifici al perimetro autorizzato, garantendo che l'utente possa accedere solo ai dati associati alla propria struttura clinica

. Le informazioni sanitarie dei pazienti sono archiviate separatamente dai risultati degli algoritmi di intelligenza artificiale.

Controllo degli accessi logici

L'accesso alle piattaforme Cloud (Folio e Tango) è regolato da connessioni sicure HTTPS e richiede un nome utente univoco, una password complessa e l'autenticazione a più fattori (MFA). I diritti di accesso sono strettamente segmentati e non esistono account generici. Le sessioni utente si disconnettono automaticamente dopo 4 ore di inattività. L'accesso al Gateway installato in ospedale per la manutenzione è protetto da VPN e segue precise policy di autenticazione in accordo con la struttura.

Tracciabilità

È garantita una tracciabilità individuale completa tramite la registrazione esaustiva (log) di tutte le richieste, gli accessi e l'utilizzo del sistema

Sicurezza dell'archiviazione digitale dei documenti

I file pseudonimizzati sono conservati all'interno dell'Unione Europea (Irlanda) su server AWS provvisti di certificazione specifica per l'Hosting di Dati Sanitari (HDS) e certificazioni ISO 27001, 27017 e 27018. L'integrità dei dati trasferiti è verificata tramite checksum e librerie dedicate. I dati vengono archiviati solo temporaneamente: al termine del periodo di conservazione autorizzato (es. 15 giorni per l'hosting AWS, 3 giorni per i partner IA), i file vengono distrutti in modo irreversibile.

Lotta contro il malware

Per impedire iniezioni di codice malevolo, gli input del sistema vengono validati rigorosamente dai framework Spring/Spring Security secondo le linee guida OWASP. Sono inoltre stati implementati processi strutturati per il monitoraggio costante e la risoluzione tempestiva delle CVE emergenti. Questo include l'analisi periodica delle dipendenze del software e l'applicazione tempestiva di patch di sicurezza per mitigare i rischi derivanti da vulnerabilità note in librerie di terze parti o componenti infrastrutturali

Sicurezza delle piattaforme e dei siti web utilizzati

I server non sono visibili direttamente su Internet; solo il servizio Folio è esposto pubblicamente ed è strettamente controllato da un API Gateway. Lo sviluppo delle piattaforme segue severe best practice di sicurezza, includendo revisioni sistematiche del codice, test di penetrazione e scansioni continue per rilevare eventuali vulnerabilità nelle dipendenze

Backup

Le immagini DICOM non vengono invece salvate in backup nel cloud in quanto, in caso di necessità o perdita, possono essere recuperate in qualsiasi momento dal server PACS del sito clinico per ripetere l'analisi.

Sicurezza dei canali informatici

Tutte le richieste API sono autenticate utilizzando JSON Web Token (JWT) di breve durata (es. validità di 1 ora per le comunicazioni tra Gateway e Folio, 5 minuti per Tango) generati dal sistema Keycloak di Identity & Access Management. Inoltre, per impedire intrusioni, non esiste alcuna connessione di rete discendente dal Cloud verso l'ospedale: è unicamente il Gateway locale ad avviare la comunicazione.

Controllo degli accessi fisici

Nessun dipendente Incepto ha accesso fisico ai server su cui sono elaborati i dati. Il sistema è suddiviso tra un Gateway locale (ospitato fisicamente presso l'infrastruttura IT dell'ospedale e quindi soggetto alle policy di sicurezza fisica della struttura clinica) e le piattaforme Cloud (Folio e Tango), che risiedono su server AWS in Irlanda. La sicurezza fisica di questi ultimi è garantita dal cloud provider (AWS), in conformità alle proprie certificazioni (tra cui ISO 27001 e HDS).

Prevenzione e Protezione contro fonti di rischio non umane

- Gestione e formazione del personale: Tutti i dipendenti Incepto lavorano all'interno dell'Unione Europea, sottoscrivono accordi di riservatezza e confidenzialità contrattuali, e ricevono regolarmente formazione in materia di privacy dei dati e sicurezza informatica, come previsto dal Sistema di Gestione della Qualità aziendale. Le loro competenze vengono valutate e aggiornate continuamente tramite specifiche procedure HR.

    - Revisione dei privilegi logici: La gestione degli accessi segue rigidi principi organizzativi: ogni accesso è soggetto ad autorizzazione esplicita, non esistono account generici o condivisi e l'autenticazione a più fattori (MFA) è implementata ovunque sia possibile. I diritti e gli accessi vengono immediatamente revocati al momento dell'uscita di un dipendente o rivisti in caso di cambio di ruolo. È inoltre prevista una riunione mensile sulla sicurezza informatica appositamente dedicata al controllo e alla revisione periodica di tutti gli accessi.

Protezione contro fonti di rischio non umane

- Le infrastrutture cloud non sono collocate in aree soggette a rischi di disastri ambientali.
- L'azienda implementa un piano di *Disaster Recovery* (ripristino di emergenza) assicurato tramite il servizio di storage AWS S3 per tutelare la continuità del servizio.
- Incepto adotta un Information Security Management System (ISMS) certificato ISO 27001, C5 ed ENS. Inoltre, il processo di progettazione e sviluppo delle piattaforme si attiene rigorosamente allo standard ISO 14971 (Gestione dei rischi dei dispositivi medici), che valuta sistematicamente e mitiga i rischi per la sicurezza dei pazienti, inclusi quelli di natura informatica (cyber-security).

Gestione postazioni

- Infrastruttura di elaborazione: il Gateway viene ospitato su una VM integrata nella policy di gestione server della struttura clinica. I servizi Cloud (Folio, Tango) sono invece ospitati in ambienti Cloud strettamente conformi ai requisiti per l'Hosting di Dati Sanitari (HDS).

- Amministrazione sicura: Gli amministratori tecnici di Incepto possono operare sulle macchine e accedere ai dispositivi e agli strumenti di gestione unicamente autenticandosi tramite MFA e instradando le comunicazioni attraverso VPN sicure

Altra misura di sicurezza fisica e/o organizzativa

- Gestione rigorosa dei Fornitori (Sub-processors): Incepto valuta accuratamente i propri partner tecnologici e i produttori di algoritmi IA tramite "Technical and Security Assessment". A tutela del trattamento, stipula con ciascuno accordi di qualità e rigorosi *Data Processing Agreement* (DPA) che li vincolano alle normative GDPR e a severi standard di sicurezza per lo sviluppo software e la protezione dei dati.
- Gestione degli incidenti (Incident Management): Il Sistema di Gestione della Qualità (certificato ISO 13485) include procedure formali per la gestione tempestiva di incidenti informatici, reclami e potenziali Data Breach (violazioni dei dati), centralizzando le comunicazioni tramite i contatti istituzionali per il supporto e la privacy (es. dpo@incepto-medical.com)

Rischi

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

mancanza di disponibilità del dato, limitazione di diritti, possibile decifratura dei dati psedonimizzati.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

azioni non autorizzate

Quali sono le fonti di rischio?

fonti umane esterne e interne

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Pseudonimizzazione, Partizionamento, Controllo degli accessi logici, Tracciabilità

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile

Rischi

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

mancanza di disponibilità del dato e limitazione di diritti

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Azioni non autorizzate

Quali sono le fonti di rischio?

Attacchi informatici

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Pseudonimizzazione, Controllo degli accessi logici, Lotta contro il malware, Backup

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile

Rischi

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Mancanza di disponibilità del dato e limitazione di diritti

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Azioni non autorizzate

Quali sono le fonti di rischio?

Attacchi informatici

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Pseudonimizzazione, Controllo degli accessi logici, Lotta contro il malware, Backup

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile

Rischi

Panoramica dei rischi

IL DIRETTORE GENERALE

Dott. Angelo Aliquò