SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI

A.A. 2025-26

Ing. Paolo Querci

ING-INF-05

Lezione 7

Perché la cybersecurity è centrale in sanità

La sanità è uno dei settori più esposti agli attacchi informatici perché gestisce **dati clinici altamente sensibili** e non può permettersi interruzioni operative

Un blocco del PACS, del RIS o dei sistemi amministrativi impedisce di eseguire e consultare esami, generando un impatto diretto sulla continuità assistenziale

I dati sanitari hanno inoltre un valore molto elevato nel mercato illegale, poiché contengono informazioni anagrafiche e cliniche difficili da sostituire

Gli attaccanti sfruttano spesso il comportamento degli utenti – email ingannevoli, allegati sospetti, credenziali deboli – più che vulnerabilità tecniche

Una singola azione errata può compromettere l'intera rete aziendale

Comprendere queste dinamiche non richiede competenze informatiche avanzate: significa adottare abitudini prudenti e riconoscere situazioni rischiose, consapevoli che la sicurezza informatica è una componente essenziale della **sicurezza del paziente**.

Phishing, malware e ransomware: cosa fanno realmente

Il **phishing** è una tecnica che imita comunicazioni legittime per convincere l'utente a rivelare credenziali o informazioni sensibili, spesso tramite email che sembrano provenire da servizi aziendali o istituzionali

Il **malware** comprende software creati per danneggiare sistemi, sottrarre dati o aprire accessi nascosti utilizzabili dagli attaccanti

Il **ransomware** è oggi la minaccia più grave: cifra interi server, inclusi PACS, RIS e repository clinici, rendendo impossibile visualizzare o refertare le immagini

Molti ospedali nel mondo hanno dovuto sospendere esami diagnostici a causa di questi attacchi

Queste minacce sfruttano comportamenti quotidiani, come aprire allegati insoliti o collegare dispositivi USB sconosciuti, ed è per questo che la prevenzione rimane l'arma più efficace per ridurre il rischio complessivo.

Perché gli ospedali sono il bersaglio preferito

Gli ospedali rappresentano un obiettivo privilegiato per i criminali informatici perché devono garantire continuità assistenziale e non possono permettersi blocchi operativi

I **dati sanitari** hanno un valore molto elevato sul mercato illegale poiché contengono informazioni cliniche e anagrafiche difficili da ricostruire

Le infrastrutture sanitarie sono spesso composte da sistemi eterogenei sviluppati in periodi diversi e questo crea vulnerabilità tecniche difficili da monitorare

Inoltre migliaia di operatori interagiscono ogni giorno con i sistemi informatici aziendali, aumentando la superficie di attacco e il rischio di comportamenti inconsapevoli

Una sola credenziale compromessa può permettere all'attaccante di muoversi all'interno della rete fino a raggiungere sistemi critici come PACS o repository documentali.

Errori comuni che espongono a rischi

Molti incidenti informatici derivano da abitudini operative diffuse ma rischiose, come l'uso di **password deboli o riutilizzate in più servizi**

L'apertura di allegati provenienti da mittenti sconosciuti, l'accesso a link non verificati e **l'utilizzo di dispositivi USB non controllati** rappresentano vettori di attacco molto frequenti

Anche l'invio di immagini cliniche tramite strumenti non sicuri come WhatsApp comporta perdita di metadati, violazioni della privacy e rischi legali

Postazioni non bloccate, aggiornamenti mancanti e dispositivi personali non protetti aumentano ulteriormente l'esposizione dell'azienda sanitaria

Conoscere questi comportamenti e correggerli riduce in modo significativo la probabilità di compromettere dati e sistemi clinici essenziali.

Buone pratiche per proteggere dati e sistemi

Una protezione efficace dei dati clinici parte da comportamenti semplici ma rigorosi, come l'uso di credenziali robuste e della **doppia autenticazione (2FA)** quando disponibile

Effettuare aggiornamenti regolari del sistema operativo e delle applicazioni riduce molte vulnerabilità note

È fondamentale verificare sempre la provenienza delle email e diffidare di richieste inattese di credenziali o allegati urgenti

Le connessioni remote devono avvenire solo tramite **VPN** aziendale e l'archiviazione dei dati deve seguire procedure ufficiali senza ricorrere a supporti esterni non autorizzati

Salvare immagini e documenti solo all'interno dei repository approvati contribuisce a mantenere tracciabilità, sicurezza e conformità normativa.

Backup, continuità operativa e ripristino

La protezione dei dati clinici richiede strategie di **backup** affidabili che permettano di recuperare immagini, referti e configurazioni essenziali anche in caso di attacco informatico

Un backup efficace deve essere conservato in copie multiple, incluse versioni offline non raggiungibili da malware o ransomware

La **continuità operativa** in sanità è fondamentale: reparti diagnostici, pronto soccorso e ambulatori devono poter continuare l'attività anche durante malfunzionamenti dei sistemi informatici

Piani di **disaster recovery** ben strutturati consentono all'azienda sanitaria di ripristinare rapidamente PACS, RIS e cartelle cliniche digitali

La capacità di riprendere l'attività senza perdere dati è un elemento chiave della sicurezza del paziente.

Domande guida: sicurezza informatica

Domanda 1. Come verificare se una comunicazione è autentica prima di cliccare su link o allegati

Domanda 2. Chi contattare in caso di dubbio su una email o un messaggio sospetto

Domanda 3. Quali comportamenti quotidiani riducono il rischio di incidenti informatici in reparto

Domanda 4. Perché la sicurezza informatica dipende in larga parte dal comportamento degli operatori

Risposte commentate: sicurezza informatica

Domanda 1. Come verificare se una comunicazione è autentica prima di cliccare su link o allegati. **Risposta.** Controllando il mittente reale, diffidando di richieste urgenti e verificando tramite canali ufficiali interni

Domanda 2. Chi contattare in caso di dubbio su una email o un messaggio sospetto. **Risposta.** L'ufficio IT o il referente aziendale per la sicurezza informatica

Domanda 3. Quali comportamenti quotidiani riducono il rischio di incidenti informatici in reparto. **Risposta.** Uso di password robuste, attenzione agli allegati, blocco delle postazioni incustodite

Domanda 4. Perché la sicurezza informatica dipende in larga parte dal comportamento degli operatori. **Risposta.** Perché gli attacchi sfruttano errori umani come fretta e distrazione

Introduzione al GDPR in ambito sanitario

Il **GDPR**[1] disciplina la protezione dei dati personali e definisce i criteri con cui devono essere trattati i **dati sanitari**, che rientrano nelle categorie a tutela rafforzata

In ambito sanitario il GDPR richiede particolare attenzione perché i dati raccolti riguardano diagnosi, esami, terapie e informazioni estremamente sensibili

I principi fondamentali includono **liceità**, **correttezza**, **trasparenza**, **minimizzazione, integrità e riservatezza.**

Ogni trattamento deve avere una finalità chiara e documentata e l'accesso deve essere limitato agli operatori autorizzati

Comprendere questi principi permette agli igienisti di lavorare in sicurezza e conformità normativa.

1. Regolamento generale sulla protezione dei dati in sigla RGPD (o GDPR in inglese General Data Protection Regulation)[2], ufficialmente regolamento (UE) n. 2016/679.

Principi fondamentali del GDPR

Liceità, correttezza e trasparenza. I dati personali devono essere trattati in modo lecito, secondo una base giuridica valida, in maniera corretta e trasparente nei confronti dell'interessato. Il paziente deve poter comprendere come e perché i suoi dati vengono utilizzati.

Minimizzazione dei dati. Devono essere raccolti e trattati solo i dati realmente necessari per la finalità clinica o amministrativa. Raccogliere o conservare informazioni non pertinenti aumenta i rischi senza apportare benefici.

Integrità e riservatezza. I dati devono essere protetti da accessi non autorizzati, perdita o distruzione, attraverso misure tecniche e organizzative adeguate. La sicurezza riguarda sia i sistemi informatici sia il comportamento degli operatori.

Titolare del trattamento: ruolo e responsabilità

Il **Titolare del trattamento** è la persona fisica o giuridica, l'autorità pubblica o altro organismo che, da solo o insieme ad altri, decide **perché** e **come** vengono trattati i dati personali e sanitari, definendo finalità, modalità operative e strumenti utilizzati

È responsabile dell'adozione di misure tecniche e organizzative adeguate per garantire sicurezza, riservatezza e corretto utilizzo dei dati

Le istruzioni fornite dal Titolare orientano l'attività quotidiana degli operatori, che trattano i dati nell'ambito delle finalità cliniche e amministrative stabilite

Comprendere questo ruolo aiuta a capire perché procedure, sistemi informativi e regole interne devono essere sempre rispettati.

Responsabile del trattamento: quando interviene

Il **Responsabile del trattamento** è un soggetto esterno che tratta dati per conto del Titolare, come fornitori di software, servizi cloud, PACS o piattaforme di telemedicina

Non decide finalità e modalità del trattamento ma deve applicare rigorosamente le istruzioni ricevute, garantendo sicurezza, formazione del personale e procedure documentate

Per gli operatori sanitari questo significa che alcuni sistemi utilizzati quotidianamente sono gestiti da Responsabili esterni, che devono assicurare qualità del servizio, protezione dei dati e tracciabilità delle operazioni.

Il DPO: garante interno della protezione dei dati

Il **Data Protection Officer (DPO)** è una figura indipendente che supporta il Titolare nella corretta applicazione del GDPR e nel monitoraggio della conformità

Non svolge funzioni disciplinari ma fornisce pareri, raccomandazioni e attività di formazione

È inoltre punto di contatto con il **Garante per la protezione dei dati personali**

Per gli operatori sanitari il DPO rappresenta un riferimento sicuro per chiarire dubbi, segnalare rischi o ricevere indicazioni su trattamenti complessi, senza timore di conseguenze personali.

Data breach e obbligo di segnalazione

Un **data breach** è qualsiasi violazione della sicurezza che comporti perdita, alterazione, divulgazione o accesso non autorizzato ai dati sanitari

Esempi comuni includono email inviate per errore a destinatari sbagliati, referti aperti da utenti non autorizzati, dispositivi smarriti o errori di caricamento nel FSE

La normativa richiede la **segnalazione immediata** al referente interno o al DPO, perché il Titolare deve valutare il rischio e notificare il Garante entro 72 ore se necessario

La tempestività della segnalazione è fondamentale per ridurre il danno e adempiere agli obblighi di legge.

Dati sanitari: cosa sono e perché sono delicati

I **dati sanitari** comprendono qualsiasi informazione relativa allo stato di salute fisica o mentale di una persona, inclusi esami diagnostici, immagini radiologiche, referti, anamnesi e terapie

Si tratta di dati che, se divulgati o utilizzati impropriamente, possono causare danni significativi alla privacy e alla dignità della persona

Per questo il GDPR impone misure di protezione più rigorose rispetto ai dati comuni

Nel lavoro quotidiano ciò significa che ogni immagine, documento o informazione clinica deve essere trattata con attenzione, evitando copie non autorizzate, canali non sicuri e condivisioni non necessarie

La tutela di questi dati è parte integrante della responsabilità professionale.

Principi di minimizzazione e tracciabilità

Il principio di **minimizzazione** stabilisce che devono essere raccolti e trattati solo i dati strettamente necessari allo scopo clinico, evitando duplicazioni o archiviazione superflua

Questo riduce il rischio di esposizione e semplifica la gestione della privacy

Il principio di **tracciabilità** richiede che ogni accesso ai dati sanitari sia registrato tramite **log** che permettono di verificare chi ha consultato o modificato referti e immagini

Questa registrazione non è solo un obbligo normativo ma uno strumento di protezione per pazienti e operatori

La tracciabilità garantisce infatti che ogni utilizzo dei dati sia giustificabile, verificabile e conforme ai protocolli aziendali.

Ruolo operativo dell’operatore sanitario

L’operatore sanitario è un **soggetto autorizzato**, abilitato a trattare dati sanitari solo quando necessario per la propria attività clinica o amministrativa

È tenuto a rispettare le misure di sicurezza, a usare esclusivamente strumenti aziendali e a mantenere la riservatezza

Non è consentito salvare dati su supporti personali, inviare immagini tramite applicazioni non autorizzate o accedere a informazioni non pertinenti al caso clinico

La base giuridica del trattamento è l’erogazione della prestazione sanitaria, quindi non serve consenso per le attività cliniche: serve invece correttezza, prudenza e rispetto delle procedure interne.

Responsabilità dell’operatore sanitario

Ogni accesso ai dati sanitari comporta una **responsabilità diretta** da parte dell’operatore, che deve utilizzare le informazioni esclusivamente per finalità connesse all’assistenza del paziente

Accedere ai dati senza motivo clinico costituisce una violazione grave, sia sul piano deontologico sia su quello legale

Gli operatori devono inoltre assicurarsi che le immagini diagnostiche, i referti e i documenti sensibili siano utilizzati solo tramite i sistemi autorizzati

Condividere informazioni tramite email personali, chat non protette o dispositivi privati espone l’azienda sanitaria a rischi elevati

La responsabilità dell’operatore si estende anche alla corretta custodia delle credenziali e alla segnalazione immediata di eventuali anomalie o incidenti di sicurezza.

DPIA: valutazione di impatto sulla protezione dei dati

La **DPIA (Data Protection Impact Assessment)** è una valutazione preventiva che il titolare del trattamento deve effettuare quando un trattamento, soprattutto se basato su **nuove tecnologie**, può comportare **rischi elevati per i diritti e le libertà delle persone fisiche** (art. 35 GDPR)

Consente di **descrivere il trattamento**, valutarne necessità e proporzionalità, **stimare probabilità e impatto dei rischi** e definire misure tecniche e organizzative di mitigazione, dimostrando la conformità normativa.

La DPIA è richiesta in particolare per **trattamenti complessi o su larga scala**, come dati sanitari, telemedicina, cloud, AI e integrazione con il FSE.

Per gli operatori significa lavorare in un contesto **analizzato ex ante**, più sicuro, trasparente e governato, a supporto di audit e controlli.

IL RISCHIO

- Il rischio è la **possibilità** che un **evento negativo** o incerto influisca sugli obiettivi di un progetto o di un'organizzazione.
- Include sia la **probabilità** che l'evento si verifichi sia l'**impatto** (negativo) che avrebbe.
- La valutazione dei rischi rappresenta un elemento chiave in molteplici contesti, inclusi la gestione dei dati, la pianificazione della risposta agli eventi avversi e la gestione dei progetti (Project Management).

Stima del Rischio: Guida Passo - Passo

- 1. **Identificazione dei Rischi**: rilevare potenziali rischi che possono influenzare il progetto o l'attività. Documentare i rischi con descrizioni dettagliate.
- 2. **Valutazione della Probabilità**: stimare la probabilità che ogni rischio si verifichi. Usare una scala qualitativa o quantitativa (es. bassa, media, alta) o percentuali. Se si vuole calcolare quantitativamente l'impatto, assegnare un valore, tipicamente da 0 (impossibilità) a 1 (certezza)
- 3. **Valutazione dell'Impatto**: determinare l'impatto che ogni rischio avrebbe se si verificasse. Usare una scala qualitativa o quantitativa (es. basso, medio, alto) o una scala numerica (1-5), quest'ultima è necessaria se si vuole calcolare quantitativamente l'impatto.

Stima del Rischio: Guida Passo per Passo

- 4. **Calcolo del Rischio**: Applica la formula per calcolare il rischio:

$$\text{Rischio} = \text{Probabilità} \times \text{Impatto}$$

Esempio di calcolo: Probabilità: 0,3 (30%), Impatto: 4 (su scala 1-5), Rischio: 0,3×4=1,20,3×4=1,2 (su scala 1-5)

- 5. **Prioritizzazione dei Rischi**: Ordina i rischi in base al valore calcolato. Focalizzati sui rischi con il punteggio più alto per adottare misure preventive e mitigative.

Rischio	Probabilità	Impatto	Rischio (P × I)
Ritardo Forniture	0,4	3	1,2
Problema Tecnico	0,2	5	1,0
Mancanza Personale	0,5	2	1,0

STIMA DEL RISCHIO: GUIDA PASSO PER PASSO

- 6. **Pianificazione delle Risposte**: Definisci le azioni per ridurre la probabilità o l'impatto dei rischi principali.Implementa strategie di mitigazione e monitoraggio continuo.

  Le **risposte** possibili sono:

  - **Evitamento**
  - **Mitigazione**
  - **Trasferimento**
  - **Accettazione**
  - **Riduzione**

Misure di Gestione dei Rischi

Evitamento del Rischio

Modificare il piano di azione/progetto o le attività per eliminare completamente il rischio.

Esempi:

- **Cambiare il piano** di progetto per evitare attività ad alto rischio.
- **Escludere opzioni** che presentano rischi significativi.
- Utilizzare **alternative** più sicure.

Misure di Gestione dei Rischi

Mitigazione del Rischio

Ridurre la gravità o l'impatto di un rischio, **una volta che si è verificato**.

Esempi:

- Aggiungere **controlli di qualità** per intercettare eventuali difetti.
- **Formare il personale** per migliorare la risposta agli errori.
- Implementare **piani di emergenza** per la gestione di eventuali incidenti.

Misure di Gestione dei Rischi

Trasferimento del Rischio

Spostare il rischio a una terza parte, come un assicuratore o un fornitore.

Esempi:

- Acquistare **assicurazioni** per coprire i danni finanziari.
- **Esternalizzare** attività a fornitori specializzati.
- Stipulare contratti di servizio con clausole di **responsabilità**.

Misure di Gestione dei Rischi

Accettazione del Rischio

Riconoscere il rischio e accetta le sue conseguenze senza intervento attivo.

Esempi:

- **Monitorare** il rischio senza adottare misure specifiche.
- Preparare un **piano di contingenza** per rispondere se il rischio si materializza.
- Accettare il rischio se i costi di mitigazione superano i benefici.

Misure di Gestione dei Rischi

Riduzione del Rischio

Implementare azioni per **ridurre la probabilità che il rischio si verifichi**.

Esempi:

- Adozione di pratiche di **manutenzione preventiva**.
- **Diversificazione dei fornitori**.
- **Pianificazione delle scorte**.
- **Formazione continua** del personale

Misure tecniche e organizzative nei sistemi sanitari

Il GDPR richiede che il Titolare adotti **misure tecniche e organizzative adeguate** per proteggere i dati sanitari

Le misure tecniche includono cifratura, autenticazione forte, backup sicuri, segmentazione della rete e aggiornamenti costanti

Le misure organizzative prevedono procedure documentate, formazione periodica, gestione degli accessi e verifica dei log

Per gli operatori sanitari questo si traduce in strumenti più sicuri e in procedure che devono essere conosciute e rispettate

Sicurezza tecnica e comportamento umano devono procedere insieme.

Esempi reali di incidenti nel settore sanitario

Negli ultimi anni diversi ospedali hanno subito incidenti significativi legati alla gestione dei dati

In alcuni casi referti sono stati inviati al paziente sbagliato a causa di errori di compilazione o distrazione

Altre volte accessi impropri alle cartelle cliniche hanno richiesto audit interni e segnalazioni al Garante

Alcune strutture hanno subito blocchi del **PACS** a causa di ransomware, con sospensione temporanea degli esami diagnostici

Questi episodi mostrano come gli incidenti non derivino solo da attacchi esterni ma anche da comportamenti quotidiani non corretti.

Cosa fare in caso di incidente o anomalia

Quando si rileva un’anomalia, come un accesso improprio, un file inviato per errore o un sospetto malware, la regola principale è **non ignorare** la situazione

È necessario interrompere l’azione, avvisare tempestivamente il referente interno o il DPO e seguire le procedure aziendali di escalation

La segnalazione rapida permette di limitare il danno, attivare indagini tecniche e adempiere agli obblighi di legge

L’operatore non deve trovare soluzioni individuali ma deve affidarsi ai canali ufficiali di gestione degli incidenti, che esistono proprio per proteggere pazienti e professionisti.

Conservazione di immagini e referti

Le immagini radiologiche e i referti devono essere archiviati in sistemi dedicati, come **PACS** e repository documentali aziendali, che garantiscono sicurezza, tracciabilità e integrità dei dati

Copie locali su PC, chiavette USB o dispositivi personali non sono consentite perché rendono impossibile controllare chi accede ai dati e impediscono il rispetto delle politiche di conservazione

Le immagini in formato DICOM includono metadati clinici che verrebbero persi se convertiti in formati non standard come JPEG o PNG

La corretta conservazione assicura che il percorso diagnostico rimanga completo, verificabile e conforme alle normative vigenti, tutelando sia il paziente sia il professionista.

Domande guida: GDPR e responsabilità

Domanda 1. Chi deve essere informato per primo in caso di errore o incidente sui dati

Domanda 2. Perché è importante segnalare subito anche errori apparentemente minori

Domanda 3. Qual è il ruolo del Titolare del trattamento

Domanda 4. Qual è il ruolo del DPO

Domanda 5. In che modo la tempestività tutela l'operatore sanitario

Risposte commentate: GDPR e responsabilità

Domanda 1. Chi deve essere informato per primo in caso di errore o incidente sui dati. **Risposta.** Il referente interno o il DPO, evitando soluzioni autonome

Domanda 2. Perché è importante segnalare subito anche errori apparentemente minori. **Risposta.** Per consentire al Titolare di valutare correttamente il rischio e adempiere agli obblighi di legge

Domanda 3. Qual è il ruolo del Titolare del trattamento. **Risposta.** Decide finalità e modalità del trattamento e le azioni operative

Domanda 4. Qual è il ruolo del DPO. **Risposta.** Supporta il Titolare dal punto di vista normativo e consulenziale

Domanda 5. In che modo la tempestività tutela l'operatore sanitario. **Risposta.** Dimostra diligenza professionale e riduce conseguenze disciplinari

Cos’è la telemedicina

La **telemedicina** comprende servizi sanitari erogati a distanza tramite sistemi informatici e di comunicazione

Non sostituisce la visita in presenza, ma permette consulenze, valutazioni e scambi clinici in situazioni in cui il paziente o il professionista non possono trovarsi nello stesso luogo

La telemedicina richiede strumenti affidabili e protocolli chiari per garantire qualità, sicurezza e riservatezza dei dati

In odontoiatria può essere utile per condividere immagini, valutare casi complessi o confrontarsi con specialisti

È fondamentale ricordare che la telemedicina è un atto sanitario a tutti gli effetti e richiede quindi attenzione alle normative sulla privacy e alla qualità delle informazioni trasmesse.

Cos’è la telemedicina

Televisita: atto sanitario in cui **il medico interagisce a distanza con il paziente**. L’atto sanitario di diagnosi che scaturisce dalla visita può dar luogo alla prescrizione di farmaci o di cure. Durante la Televisita un operatore sanitario, che si trovi vicino al paziente, può assistere il medico. Il collegamento deve consentire di vedere e interagire con il paziente e deve avvenire in tempo reale o differito.

Teleconsulto: **indicazione di diagnosi e/o di scelta di una terapia senza la presenza fisica del paziente. Si tratta di un’attività di consulenza a distanza fra medici** che permette a un medico di chiedere il consiglio di uno o più medici, in ragione di specifica formazione e competenza, sulla base di informazioni mediche legate alla presa in carico del paziente.

Cos’è la telemedicina

Telecooperazione sanitaria: atto consistente nell’**assistenza fornita da un medico o altro operatore sanitario ad un altro medico o altro operatore sanitario impegnato in un atto sanitario**. Il termine viene anche utilizzato per la consulenza fornita a quanti prestano un soccorso d’urgenza.

Quando è utile il teleconsulto odontoiatrico

Il **teleconsulto** è particolarmente utile quando è necessario ottenere rapidamente un parere specialistico su immagini diagnostiche, come radiografie endorali o CBCT

Può facilitare la collaborazione tra odontoiatri, igienisti dentali e radiologi, soprattutto nei casi in cui il paziente presenta lesioni sospette, complicazioni post-operatorie o dubbi sulla qualità dell'immagine acquisita

Il teleconsulto non sostituisce la diagnosi in presenza, ma permette di orientare correttamente il percorso clinico e di evitare ritardi inutili

Per essere efficace deve includere immagini in formato DICOM, informazioni cliniche essenziali e canali di trasmissione sicuri che garantiscano la protezione dei dati.

Cosa si trasmette in un teleconsulto

Nel teleconsulto odontoiatrico vengono trasmessi principalmente **file DICOM**, che contengono sia l'immagine sia i metadati necessari alla corretta interpretazione clinica

In alcuni casi possono essere condivise anche immagini fotografiche di supporto, purché tramite canali sicuri e solo quando strettamente necessario

È fondamentale includere una breve **scheda clinica** che descriva i sintomi, il motivo dell'esame e le informazioni utili alla valutazione

L'accuratezza dei dati trasmessi incide direttamente sulla qualità del parere specialistico

L'uso di formati non standard come JPEG compromette i metadati e può portare a valutazioni incomplete o errate, per questo deve essere evitato nei teleconsulti formali.

Requisiti tecnici per la telemedicina

Un servizio di telemedicina richiede una connessione stabile, con banda sufficiente per trasmettere **file DICOM** senza perdita di qualità o interruzioni

È necessario utilizzare piattaforme autorizzate che garantiscano cifratura, autenticazione degli utenti e tracciabilità delle operazioni

I dispositivi utilizzati per la consultazione devono essere protetti da password robuste, aggiornati e conformi alle policy aziendali

In ambito odontoiatrico, la corretta visualizzazione delle immagini richiede monitor adeguati e software compatibili con il formato DICOM

L'insieme di questi requisiti garantisce affidabilità clinica e tutela dei dati sensibili.

Rischi della telemedicina se mal gestita

Una gestione impropria della telemedicina può comportare rischi significativi, tra cui la perdita di riservatezza, l'alterazione dei dati e l'uso di immagini incomplete o non diagnostiche

L'invio di file tramite strumenti non autorizzati, come email personali o applicazioni di messaggistica, espone a violazioni del GDPR e può compromettere la qualità delle informazioni

Anche un teleconsulto basato su immagini convertite in formati non standard può portare a interpretazioni errate

Errori di identificazione del paziente o mancanza di metadati possono confondere il processo diagnostico

Per questo la telemedicina richiede rigore, procedure chiare e strumenti adeguati.

Telemonitoraggio e nuove forme di assistenza

Il **telemonitoraggio** permette di seguire il paziente a distanza attraverso la raccolta strutturata di dati clinici, immagini o parametri misurati periodicamente

In odontoiatria può supportare il follow-up post-operatorio, la valutazione dell'evoluzione di lesioni e il controllo dell'igiene orale nei pazienti più fragili

I sistemi di telemonitoraggio devono garantire sicurezza dei dati, tracciabilità e integrazione con i percorsi clinici

Pur non sostituendo la visita in presenza, consentono di individuare tempestivamente problemi che richiedono interventi più urgenti

Queste tecnologie stanno diventando parte del modello di cura moderno, anche in ambito odontoiatrico.

Domande guida: telemedicina

Domanda 1. Quali informazioni minime devono accompagnare un teleconsulto clinico

Domanda 2. Perché il formato DICOM è preferibile rispetto a immagini fotografiche

Domanda 3. Come una trasmissione impropria può influire sulla qualità della valutazione

Domanda 4. Quando è necessario rimandare il paziente alla visita in presenza

Risposte commentate: telemedicina

Domanda 1. Quali informazioni minime devono accompagnare un teleconsulto clinico. **Risposta.** Identificazione del paziente, contesto clinico e immagini diagnostiche adeguate

Domanda 2. Perché il formato DICOM è preferibile rispetto a immagini fotografiche. **Risposta.** Perché preserva qualità e metadati essenziali

Domanda 3. Come una trasmissione impropria può influire sulla qualità della valutazione. **Risposta.** Può portare a interpretazioni errate o incomplete

Domanda 4. Quando è necessario rimandare il paziente alla visita in presenza. **Risposta.** Quando le informazioni disponibili non sono sufficienti per una valutazione affidabile

Integrating the Healthcare Enterprise® (IHE)

Integrating the Healthcare Enterprise (IHE) è un'iniziativa internazionale promossa da professionisti sanitari e industria con l'obiettivo di migliorare il modo in cui i sistemi informatici in sanità **condividono le informazioni**.

IHE non è una tecnologia né un software, ma un'iniziativa organizzativa e concettuale che, mediante i **profili di integrazione**, traduce bisogni clinici in regole operative per l'uso degli standard informatici sanitari.

Integrating the Healthcare Enterprise® (IHE)

I profili IHE non sono nuovi standard, ma specifiche operative che descrivono come utilizzare standard esistenti per risolvere casi d'uso clinici concreti.Oppure ancora più semplice:Un profilo IHE è una ricetta condivisa per far funzionare davvero insieme sistemi sanitari diversi.

I sistemi che implementano i **IHE Integration Profiles** lavorano meglio insieme, risultano più semplici da integrare e permettono agli operatori sanitari di utilizzare l'informazione in modo più efficace. Il fine ultimo di IHE è l'erogazione **efficiente di cure ottimali per il paziente**.

Oggi diverse centinaia di prodotti sanitari supportano uno o più profili IHE, a dimostrazione di un'adozione ampia e consolidata a livello internazionale.

IHE: i Domini

IHE è organizzata in **Domains**, ciascuno dei quali affronta un insieme specifico di problemi e necessità all'interno di un'area clinica o infrastrutturale. I domini riflettono la complessità del sistema sanitario e permettono di sviluppare profili di integrazione mirati e coerenti.

Tra i domini attivi troviamo: **Devices (DEV) Endoscopy (ENDO)**, **IT Infrastructure (ITI)**, **Pathology and Laboratory Medicine (PaLM)**, **Patient Care Coordination (PCC)**, **Pharmacy (PHARM)**, **Quality, Research and Public Health (QRPH)**, **Radiation Oncology (RO)** e **Radiology (RAD)**.

Accanto a questi, esistono anche domini attualmente inattivi o meno sviluppati, come **Cardiology (CARD)**, **Dental (DENT)**, **Eye Care (EYECARE)** e **Surgery (SURG)**.

La struttura a domini chiarisce come IHE non sia un progetto limitato a una singola disciplina, ma un ecosistema ampio, capace di adattarsi alle esigenze di diversi ambiti della sanità.

Il dominio IHE Radiology (RAD)

Il dominio **IHE Radiology (RAD)** affronta i bisogni informativi specifici della radiologia diagnostica, un'area caratterizzata da grande produzione di immagini e documenti.

L'obiettivo è assicurare che immagini, referti e dati correlati siano disponibili nel punto di cura, utilizzando formati e procedure standardizzate.

RAD consiste di (definisce) un insieme di **profili** che riguardano l'intero processo radiologico, dal momento della richiesta dell'esame alla produzione e distribuzione dei risultati, favorendo una radiologia **coerente, tracciabile e interoperabile** tra reparti e strutture diverse.

Profili e flussi nel dominio RAD

Tra i profili più rilevanti del dominio **RAD** troviamo quelli che regolano la gestione delle immagini e dei referti, come l'uso corretto del formato **DICOM**, l'allineamento tra richieste esaminate e studi prodotti e la condivisione dei risultati con sistemi esterni.

Questi profili guidano l'interazione tra **RIS**, **PACS** e altri sistemi clinici, assicurando che ogni immagine sia correttamente identificata, archiviata e resa disponibile per la consultazione.

Nel contesto multi-struttura, le funzionalità RAD si estendono ulteriormente attraverso meccanismi come **XDS-I**, che consente di rendere visibile e recuperabile un esame anche al di fuori della struttura che lo ha prodotto.

XDS: significato e obiettivo

Cross Enterprise Document Sharing (XDS) è un **profilo** progettato per la **catalogazione e la condivisione dei documenti clinici** tra istituzioni sanitarie diverse.

XDS è un profilo di integrazione definito da IHE nel dominio IT Infrastructure, ma è concettualmente trasversale, perché fornisce un'infrastruttura comune per la condivisione dei documenti clinici in tutti gli ambiti della sanità.

L'obiettivo di XDS non è creare nuovi dati clinici, ma permettere che documenti già esistenti possano essere trovati e utilizzati anche al di fuori della struttura che li ha prodotti.

XDS introduce un modello comune per sapere **quali documenti esistono**, a quale paziente si riferiscono e dove sono archiviati, rendendo possibile una reale continuità informativa tra organizzazioni sanitarie.

Richiami sulll'Intelligenza Artificiale in sanità

L'**Intelligenza Artificiale** è un insieme di tecniche che permettono ai sistemi informatici di analizzare dati complessi e individuare pattern utili al supporto decisionale clinico

Non sostituisce l'operatore sanitario ma può assisterlo nell'interpretazione delle immagini, nell'individuazione precoce di anomalie e nel monitoraggio dei trattamenti

Nella pratica odontoiatrica l'AI può facilitare la valutazione di CBCT, radiografie endorali e fotografie cliniche

È importante comprendere che l'AI richiede dati di qualità e non è infallibile: errori di addestramento, bias nei dataset o immagini non idonee possono portare a suggerimenti non accurati

L'uso responsabile dell'AI richiede consapevolezza dei suoi limiti.

AI: detection, segmentazione e valutazione automatica

L'AI può supportare l'analisi delle immagini diagnostiche attraverso tecniche come la **detection**, che individua regioni sospette, e la **segmentazione**, che separa strutture anatomiche o lesioni per facilitarne la valutazione

Questi strumenti possono aiutare l'operatore a concentrarsi sulle aree di maggiore rilevanza clinica e ridurre il rischio di omissioni

Nelle immagini odontoiatriche l'AI può facilitare l'identificazione di lesioni periapicali, difetti ossei o variazioni anatomiche complesse

È importante ricordare che l'AI non fornisce diagnosi definitive ma un supporto che va interpretato con competenza professionale e senso critico.

Limiti dell’Intelligenza Artificiale

Nonostante i progressi, l’AI presenta **limiti strutturali** che devono essere compresi

Le prestazioni dipendono fortemente dalla qualità e dalla varietà dei dati su cui il modello è stato addestrato

Immagini rumorose, incomplete o non conformi agli standard possono generare risultati inaccurati

L’AI non comprende il contesto clinico e può produrre valutazioni errate se applicata in situazioni non previste dal suo addestramento

Inoltre alcuni modelli funzionano come “scatole nere”, rendendo difficile spiegare come venga generata una certa indicazione

Per questo l’AI deve essere considerata un supporto e non uno strumento decisionale autonomo.

Bias nei dataset e rischi di errori

I **bias nei dataset** possono influenzare significativamente le prestazioni dell'AI

Se il modello è stato addestrato su immagini provenienti da popolazioni limitate, con caratteristiche anatomiche o patologie non rappresentative, le sue valutazioni potrebbero essere meno accurate in altri contesti

Anche la presenza di errori nei dati di addestramento può portare a risultati fuorvianti

In odontoiatria questo si traduce in possibili falsi positivi o negativi, che devono essere riconosciuti e gestiti dal professionista

La consapevolezza dei bias permette all'operatore di interpretare l'AI con maggiore prudenza e competenza.

Responsabilità clinica nell'uso dell'AI

L'uso dell'AI non modifica la responsabilità del professionista, che rimane sempre il principale decisore clinico

Gli strumenti basati su AI devono essere utilizzati come supporto alla valutazione e non come sostituti dell'interpretazione umana

È fondamentale verificare la coerenza dei suggerimenti generati dall'AI con il quadro clinico complessivo del paziente

L'operatore deve conoscere i limiti dello strumento, verificarne l'affidabilità e segnalare eventuali comportamenti anomali

La responsabilità finale sulla diagnosi e sulle decisioni terapeutiche rimane sempre in capo al professionista, indipendentemente dalle indicazioni fornite dal sistema di AI.

AI e miglioramento dei flussi clinici

Oltre all'interpretazione delle immagini, l'AI può contribuire al miglioramento dei **flussi clinici**, aiutando a organizzare informazioni, identificare priorità e ridurre errori nei passaggi di consegne

Algoritmi ben addestrati possono evidenziare anomalie nei dati, suggerire controlli aggiuntivi o segnalare pattern che potrebbero sfuggire all'attenzione umana

In odontoiatria ciò può tradursi in percorsi più rapidi nel triage dei pazienti, nel confronto con casi simili o nella verifica automatica della completezza della documentazione

L'AI non sostituisce l'organizzazione clinica, ma può renderla più efficiente e ridurre il carico cognitivo dei professionisti.

Domande guida: AI e decisione clinica

Domanda 1. Cosa fare se il suggerimento dell'AI è in contrasto con la valutazione clinica

Domanda 2. Chi mantiene la responsabilità della decisione finale

Domanda 3. Perché è importante conoscere i limiti dell'AI

Domanda 4. In quali situazioni l'AI rappresenta un reale supporto

Risposte commentate: AI e decisione clinica

Domanda 1. Cosa fare se il suggerimento dell'AI è in contrasto con la valutazione clinica. **Risposta.** Prevale sempre il giudizio dell'operatore sanitario

Domanda 2. Chi mantiene la responsabilità della decisione finale. **Risposta.** La responsabilità resta sempre in capo al professionista sanitario

Domanda 3. Perché è importante conoscere i limiti dell'AI. **Risposta.** Evita un uso acritico e improprio dello strumento

Domanda 4. In quali situazioni l'AI rappresenta un reale supporto. **Risposta.** Come supporto all'attenzione e alla coerenza, non come sostituto del ragionamento clinico

Interoperabilità: perché è necessaria in sanità

Nei contesti sanitari moderni il percorso di un paziente coinvolge **più sistemi informatici**, spesso prodotti da fornitori diversi.

Anagrafica, appuntamenti, referti testuali e immagini diagnostiche possono risiedere in sistemi separati che, senza regole comuni, non comunicano correttamente.

L'assenza di interoperabilità porta a **informazioni frammentate**, errori di trascrizione e ripetizione di esami.

L'interoperabilità consente ai sistemi di **scambiarsi dati clinici in modo sicuro, strutturato e comprensibile**, mantenendo il significato dell'informazione.

Fascicolo Sanitario Elettronico e immagini radiologiche

Il **Fascicolo Sanitario Elettronico (FSE)** raccoglie informazioni cliniche del paziente, rendendole disponibili ai professionisti autorizzati

Nel FSE possono confluire referti, esami di laboratorio, prescrizioni e talvolta anche immagini radiologiche o link ai repository che le contengono

L'obiettivo è garantire continuità assistenziale, permettendo ai clinici di consultare rapidamente dati aggiornati e contestualizzati

Per funzionare correttamente il FSE richiede integrazione con PACS e sistemi regionali, oltre a standard condivisi per i metadati

Un FSE completo riduce errori, facilita diagnosi più rapide e rende il percorso del paziente più lineare.

Competenze digitali per il professionista sanitario

L’evoluzione dei sistemi informativi sanitari richiede che i professionisti sviluppino **competenze digitali** solide, non solo nell’uso degli strumenti ma nella comprensione dei principi che li governano

Saper interpretare correttamente immagini, metadati, flussi informativi e strumenti di telemedicina aumenta la qualità dell’assistenza

Anche la capacità di riconoscere rischi informatici e applicare buone pratiche di sicurezza è parte integrante della professionalità moderna

Le competenze digitali permettono inoltre di collaborare meglio con radiologi, ingegneri clinici e personale IT, contribuendo a percorsi di cura più efficienti e sicuri.

Il futuro del lavoro sanitario digitale

Il futuro del lavoro sanitario sarà sempre più integrato con sistemi digitali intelligenti, in grado di supportare diagnosi, follow-up e gestione dei dati clinici

L'AI diventerà uno strumento abituale, affiancando i professionisti nell'analisi delle immagini e nella gestione delle informazioni

L'interoperabilità tra strutture, il cloud e la telemedicina renderanno i percorsi di cura più fluidi e accessibili

Tuttavia questa trasformazione richiede consapevolezza critica: i professionisti dovranno mantenere centralità nel processo clinico, interpretando i dati e prendendo decisioni consapevoli

La tecnologia sarà un supporto, non un sostituto della competenza umana.

Sintesi finale della lezione

La sicurezza informatica, la protezione dei dati clinici, la telemedicina e l'uso consapevole dell'AI rappresentano competenze fondamentali per l'operatore sanitario moderno

Comprendere rischi, procedure e potenzialità di questi strumenti consente di lavorare in modo sicuro, efficace e conforme alle normative

L'AI e le tecnologie digitali ampliano le possibilità diagnostiche e organizzative ma richiedono attenzione ai limiti e responsabilità professionale

La trasformazione digitale non riguarda solo i sistemi informatici ma il modo di collaborare, comunicare e assistere il paziente

Il professionista resta al centro, con strumenti più potenti e un ruolo sempre più strategico.

GRAZIE PER L'ATTENZIONE

Domande guida: sicurezza informatica

Domanda 1. Come verificare se una comunicazione è autentica prima di cliccare su link o allegati

Domanda 2. Chi contattare in caso di dubbio su una email o un messaggio sospetto

Domanda 3. Quali comportamenti quotidiani riducono il rischio di incidenti informatici in reparto

Domanda 4. Perché la sicurezza informatica dipende in larga parte dal comportamento degli operatori

Risposte commentate: sicurezza informatica

Domanda 1. Come verificare se una comunicazione è autentica prima di cliccare su link o allegati. **Risposta.** Controllando il mittente reale, diffidando di richieste urgenti e verificando tramite canali ufficiali interni

Domanda 2. Chi contattare in caso di dubbio su una email o un messaggio sospetto. **Risposta.** L'ufficio IT o il referente aziendale per la sicurezza informatica

Domanda 3. Quali comportamenti quotidiani riducono il rischio di incidenti informatici in reparto. **Risposta.** Uso di password robuste, attenzione agli allegati, blocco delle postazioni incustodite

Domanda 4. Perché la sicurezza informatica dipende in larga parte dal comportamento degli operatori. **Risposta.** Perché gli attacchi sfruttano errori umani come fretta e distrazione

Domande guida: GDPR e responsabilità

Domanda 1. Chi deve essere informato per primo in caso di errore o incidente sui dati

Domanda 2. Perché è importante segnalare subito anche errori apparentemente minori

Domanda 3. Qual è il ruolo del Titolare del trattamento

Domanda 4. Qual è il ruolo del DPO

Domanda 5. In che modo la tempestività tutela l'operatore sanitario

Risposte commentate: GDPR e responsabilità

Domanda 1. Chi deve essere informato per primo in caso di errore o incidente sui dati. **Risposta.** Il referente interno o il DPO, evitando soluzioni autonome

Domanda 2. Perché è importante segnalare subito anche errori apparentemente minori. **Risposta.** Per consentire al Titolare di valutare correttamente il rischio e adempiere agli obblighi di legge

Domanda 3. Qual è il ruolo del Titolare del trattamento. **Risposta.** Decide finalità e modalità del trattamento e le azioni operative

Domanda 4. Qual è il ruolo del DPO. **Risposta.** Supporta il Titolare dal punto di vista normativo e consulenziale

Domanda 5. In che modo la tempestività tutela l'operatore sanitario. **Risposta.** Dimostra diligenza professionale e riduce conseguenze disciplinari

Domande guida: telemedicina

Domanda 1. Quali informazioni minime devono accompagnare un teleconsulto clinico

Domanda 2. Perché il formato DICOM è preferibile rispetto a immagini fotografiche

Domanda 3. Come una trasmissione impropria può influire sulla qualità della valutazione

Domanda 4. Quando è necessario rimandare il paziente alla visita in presenza

Risposte commentate: telemedicina

Domanda 1. Quali informazioni minime devono accompagnare un teleconsulto clinico. **Risposta.** Identificazione del paziente, contesto clinico e immagini diagnostiche adeguate

Domanda 2. Perché il formato DICOM è preferibile rispetto a immagini fotografiche. **Risposta.** Perché preserva qualità e metadati essenziali

Domanda 3. Come una trasmissione impropria può influire sulla qualità della valutazione. **Risposta.** Può portare a interpretazioni errate o incomplete

Domanda 4. Quando è necessario rimandare il paziente alla visita in presenza. **Risposta.** Quando le informazioni disponibili non sono sufficienti per una valutazione affidabile

Domande guida: AI e decisione clinica

Domanda 1. Cosa fare se il suggerimento dell'AI è in contrasto con la valutazione clinica

Domanda 2. Chi mantiene la responsabilità della decisione finale

Domanda 3. Perché è importante conoscere i limiti dell'AI

Domanda 4. In quali situazioni l'AI rappresenta un reale supporto

Risposte commentate: AI e decisione clinica

Domanda 1. Cosa fare se il suggerimento dell'AI è in contrasto con la valutazione clinica. **Risposta.** Prevale sempre il giudizio dell'operatore sanitario

Domanda 2. Chi mantiene la responsabilità della decisione finale. **Risposta.** La responsabilità resta sempre in capo al professionista sanitario

Domanda 3. Perché è importante conoscere i limiti dell'AI. **Risposta.** Evita un uso acritico e improprio dello strumento

Domanda 4. In quali situazioni l'AI rappresenta un reale supporto. **Risposta.** Come supporto all'attenzione e alla coerenza, non come sostituto del ragionamento clinico