

Indice

Introduzione	3
Capitolo 1 : Stato dell'arte del sistema RIS-PACS.....	4
1.1 Sistema Informativo Sanitario.....	5
1.2 Sistema di Accettazione/Dimissione/Trasferimento.....	5
1.3 Centro Unico di Prenotazione	6
1.4 Sistema Informatico Radiologico.....	6
1.4.1 Integrazione del RIS.....	8
1.5 Picture Archiving and Communication System (PACS)	9
1.5.1 Integrazione del PACS	12
1.5.2 PACS AOU	13
1.6 Modalità diagnostiche.....	14
1.7 Workstation.....	16
Capitolo 2 : Aggiornamento del PACS	19
2.1 Obiettivi.....	19
2.2 Innovazioni	20
2.3 Architettura tecnica	21
2.4 Centricity Clinical Archive (Enterprise Archive).....	24
2.5 Centricity Zero Foot Print	24
2.6 Centricity Universal Viewer	27
2.7 Centricity SenoIris Workstation	30
2.8 Workstation di refertazione	31
2.9 Monitor Diagnostici.....	32
2.10 Centricity RA600.....	34
Capitolo 3 : Cenni di sicurezza informatica	35
3.1 Legislazione europea ed internazionale.....	35
3.2 La sicurezza informatica all'interno del processo di approvvigionamento.....	38
3.3 Standard e linee guida di settore rilevanti	39
3.4 Tassonomia delle minacce	40
3.5 Valutazione critica e applicazione del documento	44

Capitolo 4 : Norme di buon utilizzo RIS-PACS del Tecnico	
Sanitario di Radiologia Medica	53
4.1: Case Report : analisi e correzione	54
4.1.1 Caso di omonimia al Sant'Orsola di Bologna.....	54
4.1.2 Caso di errata fusione paziente presso l'Azienda Ospedaliero Universitaria Ospedali Riuniti di Ancona	59
Glossario	63
Conclusioni	65
Ringraziamenti	66
Sitografia	67
Bibliografia.....	67

Introduzione

La sicurezza informatica, in ambito medico deve essere considerata un elemento strutturale.

In ogni fase di progettazione, installazione, gestione, utilizzo e manutenzione deve essere parte integrante. Infatti i sistemi informatici, in relazione alla loro rapidissima evoluzione e alla loro complessità strutturale, sono costantemente esposti a rischi. I dispositivi medicali, gestendo dati sensibili sono a maggior ragione esposti anche ad azioni malevole esterne.

I rischi quindi, possono essere fondamentalmente individuati in due tipologie: malfunzionamenti e attacchi esterni.

I primi possono causare interruzioni di servizio e perdita di dati o errori di diverso tipo con possibili conseguenze anche sulla salute dei pazienti; gli altri ugualmente possono produrre interruzione di servizio o perdita/furto di dati anche se le finalità sono nella maggior parte delle volte a scopo di lucro.

Le difficoltà per entrambe le tipologie sono che in ambo i casi non è facilmente prevedibile individuare le caratteristiche del problema.

Per questa ragione ad ogni intervento maggiore sul sistema, come ad esempio un aggiornamento, diventa mandatorio predisporre attività pratiche e organizzative per gestire i futuri rischi.

Poiché la maggior parte dei sistemi è strettamente integrata alle architetture aziendali preesistenti, questa attività di valutazione e prevenzione del rischio si complica e necessita sia l'integrazione dei sistemi informatici, sia quella delle competenze.

In questo lavoro di tesi in previsione dell'aggiornamento del sistema PACS è stata fatta un'analisi sulle attività di risk assessment individuando competenze, attori e aree di rischio.

Capitolo 1 : Stato dell'arte del sistema RIS-PACS

Picture Archiving and Communication System (PACS) è un sistema hardware e software dedicato all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali.

Il PACS, però, è solo uno degli attori del flusso radiologico, i quali si relazionano e comunicano l'uno con l'altro tramite standard HL7 e DICOM.

E' di cruciale importanza l'integrazione del PACS con il sistema informativo radiologico (RIS), ossia il software che gestisce il flusso dell'esame radiologico dall'accettazione fino alla dimissione del paziente.

I vari attori, che permettono il normale svolgimento del workflow sono:

- Sistema di Accettazione/Dimissione/Trasferimento (ADT)
- Sistema informativo sanitario (HIS)
- Centro Unico di Prenotazione (CUP)
- Sistema Informatico Radiologico (RIS)
- Picture Archiving and Communication System (PACS)
- Workstation per la post-elaborazione
- Modalità diagnostiche (mammografo, RM, TC, endorali...)
- Reparti
- Workstation di refertazione
- Masterizzatori/Sistemi di distribuzione a esterni

E' importante vedere come tali attori, si interfacciano tra loro, utilizzando di solito i relativi profili IHE (Integrating the Healthcare Enterprise) tramite lo standard HL7 (Health Level 7).

1.1 Sistema Informativo Sanitario

Il sistema informativo sanitario (HIS) è uno strumento informatico, o meglio l'insieme integrato di strumenti informatici, utilizzati in ambito sanitario per gestire i flussi amministrativi e clinici di un ospedale.

Tipicamente esso contempla l'anagrafica centrale, l'archivio dei referti, il sistema di accettazione/dimissione/trasferimento, e l'analisi dei costi.

Si interfaccia con il sistema di ammissione/dimissione/trasferimento e con il sistema informatico radiologico.

1.2 Sistema di Accettazione/Dimissione/Trasferimento

Il sistema di Accettazione/Dimissione/Trasferimento (ADT) gestisce i pazienti ricoverati dal punto di vista prevalentemente amministrativo.

Esso può contenere anche un sistema di order-entry, deputato alla gestione del flusso di richieste di prestazioni, consulenze e servizi, dai reparti ospedalieri verso i servizi erogatori.

Monitora lo stato di avanzamento delle richieste e la gestione delle informazioni di ritorno, come ad esempio: referti, immagini non radiologiche, dati strutturati (laboratorio, microbiologia), assicurando così una corretta gestione del flusso di richiesta all'interno di una struttura sanitaria.

Il sistema di accettazione/dimissione/trasferimento si interfaccia con il CUP, in modo che il paziente dopo essere entrato nella struttura sanitaria possa richiedere una prestazione.

Dunque, l'ADT si deve interfacciare con il RIS, al fine di prenotare la prestazione sanitaria richiesta.

1.3 Centro Unico di Prenotazione

Il centro unico di prenotazione (CUP) è il sistema che rende possibile l'accesso, tramite prenotazione, alle prestazioni ambulatoriali, che siano queste istituzionali o in libera professione.

Il CUP, al fine di uniformare l'accesso alle prestazioni ed accorciare i tempi d'attesa del paziente, è strutturato su scala di area vasta o regionale ed è integrato con il sistema di cassa.

1.4 Sistema Informatico Radiologico

Il Sistema Informatico Radiologico (RIS) è un sistema informatico dedicato all'ambito radiologico, utile al fine di gestire il flusso dei dati legati ai pazienti ed alle prestazioni radiologiche.

L'utilizzo del RIS trova riscontro nella gestione delle statistiche di natura amministrativa, poiché l'introduzione dei budget implica il preciso conteggio degli esami eseguiti, e del tipo di esami svolti.

Il sistema informatico radiologico partecipa alla raccolta delle informazioni necessarie al fine di gestire nel miglior modo possibile la apparecchiature di cui dispone il reparto, vengono così stimati il carico di lavoro, le condizioni del macchinario ed i tempi di fermo-macchina.

Oltretutto, il RIS svolge un ruolo chiave all'interno di un reparto di radiologia, tramite il RIS infatti, si gestisce il processo di accettazione, di produzione delle immagini e di refertazione.

In dettaglio, il processo comincia con la richiesta d'esame, che attiva i processi del RIS, tramite il quale si recuperano una serie di informazioni di interesse clinico ed amministrativo.

Informazioni di tipo amministrativo sono l'anagrafica del paziente, il tipo di esame richiesto, la sala in cui viene svolto l'esame, l'operatore che svolge tale esame e vincoli temporali legati allo svolgimento dell'esame (eventuale urgenza o esame di routine).

Per recuperare tali dati è cruciale il dialogo del RIS con altri sistemi informativi, ad esempio il tipo di esame da effettuare può essere contenuto all'interno del sistema informativo regionale.

Invece, riguardo le informazioni di interesse clinico, esse sono essenziali al fine di risalire al motivo per cui viene richiesto l'esame.

Successivamente, tramite il RIS, si aggiorna l'agenda radiologica, in base alla disponibilità di sale, apparecchiatura e personale.

Il RIS, dopo aver verificato l'assenza di eventuali incompatibilità con l'esame richiesto, elabora un appuntamento e produce un foglio informativo, il quale viene consegnato al paziente e/o inviato al reparto, al fine di effettuare una corretta preparazione necessaria per lo svolgimento dell'esame.

Il giorno dell'esame, con l'arrivo del paziente, il RIS provvede all'accettazione del paziente, e poiché il RIS comunica con le apparecchiature diagnostiche, l'immissione dei dati del paziente su di esse, avviene automaticamente, senza alcun intervento dell'operatore, tuttavia è possibile correggere manualmente le richieste in base alle disponibilità del momento.

Tale procedimento di passaggio automatico di dati tra RIS e apparecchiature evita errori che potrebbero portare ad una distorsione delle reali informazioni.

A questo punto si procede con l'esecuzione dell'esame e quindi con la produzione delle immagini diagnostiche.

I dati relativi all'acquisizione delle immagini, come ad esempio parametri di esposizione, posizione del paziente, ed eventuale uso di MdC, sono parte integrante dell'esame; tali dati possono essere trasmessi direttamente al RIS, se le immagini prodotte sono in formato DICOM.

Dopo aver eseguito l'esame, si procede all'interpretazioni delle immagini da parte del medico Radiologo ed alla conseguente produzione del referto.

Il referto, solitamente, è composto dalla descrizione dell'esame effettuato, dal codice dell'esame, dalla descrizione dei segni radiologici rilevati sull'immagini, e dunque dalla formulazione di un'ipotesi diagnostica.

Il referto, dopo essere stato firmato digitalmente dal medico Radiologo, viene integrato ed è visualizzabile anche su PACS.

Il RIS, infine, provvede all'archiviazione, ossia alla conservazione dei dati ottenuti dall'indagine diagnostica.

Deve quindi esserci un'integrazione bidirezionale forte tra RIS e PACS.

1.4.1 Integrazione del RIS

Il sistema informatico radiologico comunica con altri sistemi informativi clinici, a monte ed a valle del flusso di lavoro radiologico.

Nello specifico il RIS riceve dati dall' ADT e dal CUP e dialoga con le modalità diagnostiche, fornendogli le credenziali anagrafiche del paziente, e con il PACS, nel quale vengono trasferite le immagine diagnostiche ad esame completato.

La comunicazione tra sistemi informativi distinti, i quali gestiscono dati anagrafici, clinici e diagnostici, a volte può risultare complessa e ricca di conflitti.

L'IHE, ossia "Integrating the Healthcare Enterprise" è un'iniziativa nata negli USA nel 1998, dalla collaborazione di RSNA (Radiological Society of North America) e HIMSS (Healthcare Information and Management Systems Society). Obiettivo di tale iniziativa è quello di definire come gli standard esistenti (DICOM ed HL7) dovevano essere impiegati dai vari sistemi informativi, al fine di realizzare un'integrazione tra loro.

Precisamente, HL7 è uno standard di messaggistica, il quale permette lo scambio di set di dati clinici ed amministrativi tra diversi applicativi sanitari. Esso fornisce uno standard per lo scambio e l'integrazione di dati, favorendo una migliore gestione clinica del paziente, ed una migliore valutazione dei servizi sanitari.

HL7 è tale, perché si pone al livello 7, nel modello ISO-OSI, in cui il livello più basso corrisponde al livello di comunicazione fisica, ed il livello più alto riguarda i programmi applicativi.

HL7, diversamente da DICOM, lavora solo su dati che possono essere scambiati con i messaggi.

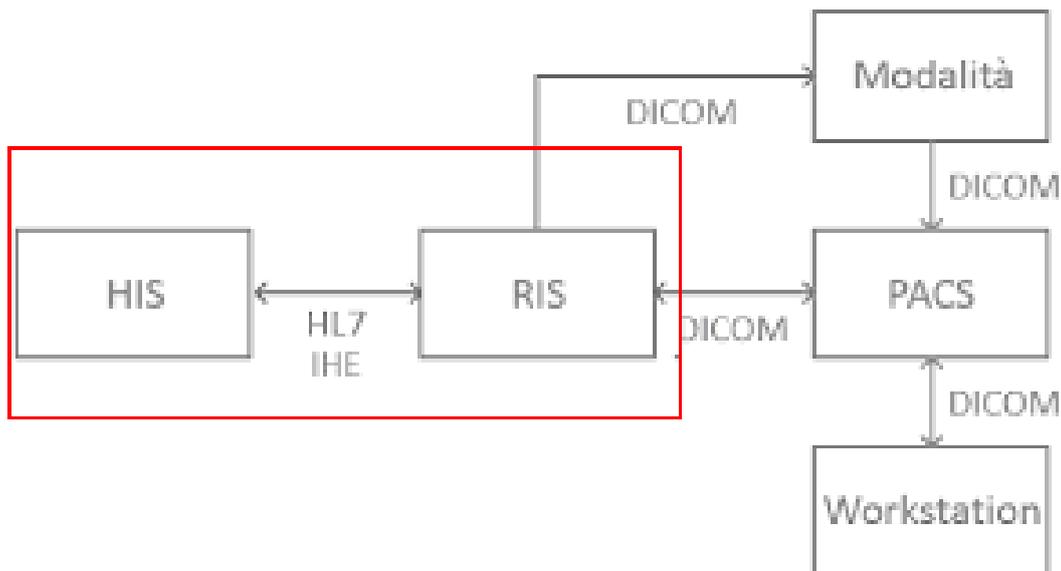


Fig.1 comunicazione tra i vari applicativi all'interno del reparto di Radiologia

1.5 Picture Archiving and Communication System (PACS)

Il PACS, ossia il sistema di archiviazione e trasmissione di immagine, come detto ad inizio capitolo, consiste in un sistema hardware e software dedicato all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali.

Secondo la direttiva CEE 93/42 sui dispositivi medici, i sistemi PACS sono da considerare dispositivi medici, in quanto il loro utilizzo è finalizzato ad ottenere una diagnosi.

Componenti principali del sistema PACS sono la parte dedicata all'archiviazione, utile ai fini della gestione dei dati e delle immagini, e la parte dedicata alla visualizzazione, la quale permette di visualizzare l'immagine diagnostica su monitor ad alta risoluzione, tramite i quali si effettua diagnosi.

Con l'evoluzione dei software, è diventato possibile anche effettuare post-elaborazione sull'immagine, come ad esempio ricostruzioni MIP, VR ed MPR.

L'introduzione del PACS ha comportato notevoli vantaggi tra cui un aumento della produttività delle apparecchiature, una riduzione del rischio di perdita delle

informazioni, ed un risparmio di tempo nella distribuzione delle immagini diagnostiche ai reparti.

Il PACS, nel suo insieme si interfaccia con componenti hardware e software, che ne permettono il funzionamento.

Si possono classificare tali componenti in base alla loro funzione in :

- dispositivi deputati all'acquisizione delle immagini provenienti dalle varie modalità diagnostiche;
- dispositivi deputati all'archiviazione delle immagini diagnostiche su supporti digitali;
- dispositivi deputati alla visualizzazione, elaborazione e stampa delle immagini, ossia le workstation, sia quelle su cui si effettua il post-processing, che quelle in cui si effettua la produzioni di referti.

Il Digital Imaging and COmmunication in Medicine è uno standard informatico utilizzato per il formato e lo scambio di immagini biomediche, nato dalla collaborazione tra la National Electrical Manufacturer Association (NEMA) e l'American College of Radiology (ACR), progettato per permettere l'interoperabilità tra apparecchiature medicali e sistemi informatici indipendentemente dal produttore, agevolando così realtà multivendor.

La versione attualmente in uso è la 3.0, nata nel 1993, nella quale sono implementati i protocolli di rete TCP/IP e OSI.

Il formato DICOM si posiziona al livello 7 della pila ISO/OSI, ed è indipendente dagli strati di comunicazione sottostanti.

Tale versione permette la comunicazione automatica tra le macchine di avvenuta ricezione del pacchetto di esame spedito, la ricezione automatica delle worklist sulla console di comando o la definizione univoca delle modalità di masterizzazione di un supporto ottico CD o DVD.

Riguardo la compressione dell'immagine lo standard DICOM non dà indicazioni, né per quanto riguarda l'algoritmo, né per il rapporto di compressione e non

raccomanda nessun tipo di formato particolare anche se il più utilizzato rimane quello “lossless”, cioè senza perdita di informazioni.

Lo standard DICOM è pubblico, di conseguenza le sue specifiche sono accessibili a tutti i produttori di medical device: la compatibilità di un dispositivo deve essere certificata dal costruttore attraverso un documento autocertificativo di dominio pubblico, denominato DICOM conformance Statement, che ne elenchi le funzionalità.

Lo standard DICOM possiede numerosi servizi, in totale 15, non tutti però utilizzati in ambiente PACS.

Ogni tipologia di immagine (CT, MR, CR etc.) presenta quindi una struttura propria, in quanto sono differenti le modalità di produzione delle stesse.

Le immagini in formato DICOM sono composte di un HEADER dove sono contenute le informazioni anagrafiche del paziente, le informazioni tecniche dell'esame (proiezione, sequenza, carichi radiologici, etc.) ed altri dati relativi all'esame (data, macchinario, diagnostica).

Dopo l' HEADER vi è la matrice numerica dell'immagine vera e propria.

La gestione dell'archiviazione dei dati, è svolta nello specifico da diversi componenti hardware, ossia:

- HL7 Broker, si occupa di garantire la comunicazione tra RIS e PACS ;
- DICOM Broker, si occupa della gestione dei servizi per la trasmissione e la ricezione delle immagini diagnostiche, oltre a gestire le worklist;
- Manager, dopo aver elaborato le richieste dei broker, si interfaccia con i database;
- WADO, Web Access to DICOM Objects, descrive in che modo accedere tramite i protocolli web (http, https) ad oggetti DICOM (immagini o referti), permette quindi di comunicare con sistemi che non utilizzano il protocollo DICOM;
- Web Server, deputato alla gestione tramite web dei servizi del server PACS;

- Datavate System, database testuale in cui sono contenute le informazioni gestite dal sistema;
- Archive Storage, complesso di dispositivi a chi è affidata la memorizzazione delle immagini diagnostiche.

1.5.1 Integrazione del PACS

Il concetto di integrazione espresso precedentemente per il RIS, viene ribadito anche per i sistemi PACS.

E' essenziale che il PACS utilizzi standard DICOM, al fine di poter interrogare, recuperare ed archiviare dati e consentire le operazioni di stampa e masterizzazione.

La trasmissione delle immagini dalle modalità al PACS ed alle workstation dipende dall'infrastruttura di rete, è essenziale che questi sistemi siano interconnessi tra loro, al fine di ottimizzare la produzione degli esami diagnostici.

Alla base di una infrastruttura valida, deve essere garantita la continuità operativa, inoltre tale infrastruttura deve essere sicura ed adatta alle performance operative.

Per ottenere una configurazione di rete efficiente devono essere considerati alcuni aspetti, tra cui il numero di nodi, la disposizione di tali nodi e le relative modalità di accesso, il livello di sicurezza, la presenza di eventuali vincoli, che possano essere economici, architettonici o legali, l'eventualità di dover procedere nel tempo ad effettuare delle modifiche ed infine, la destinazione d'uso dei locali (modalità, workstation, reparti e PACS).

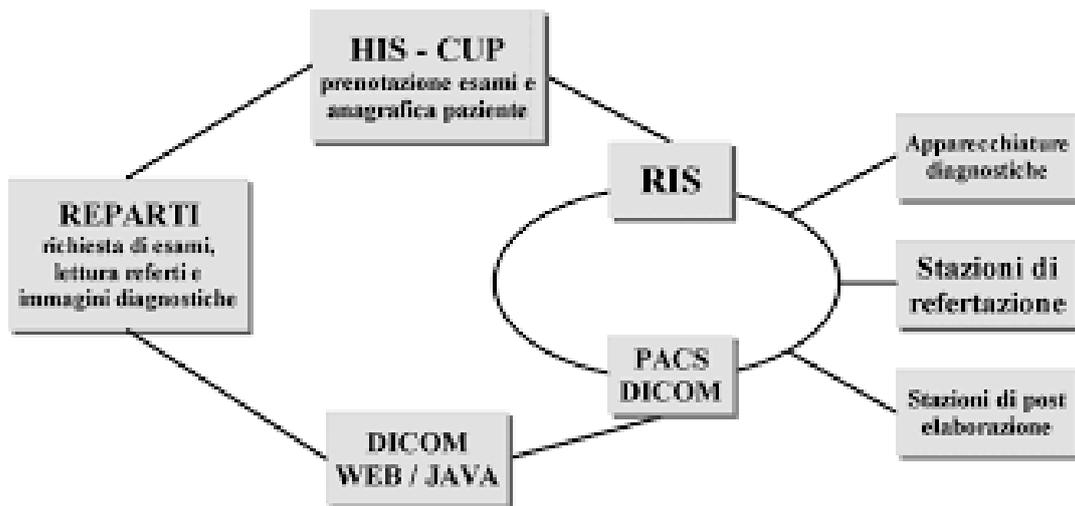


Fig.2 Interfaccia tra PACS e workstation di refertazione e postelaborazione, modalità radiologiche e client RIS.

1.5.2 PACS AOU

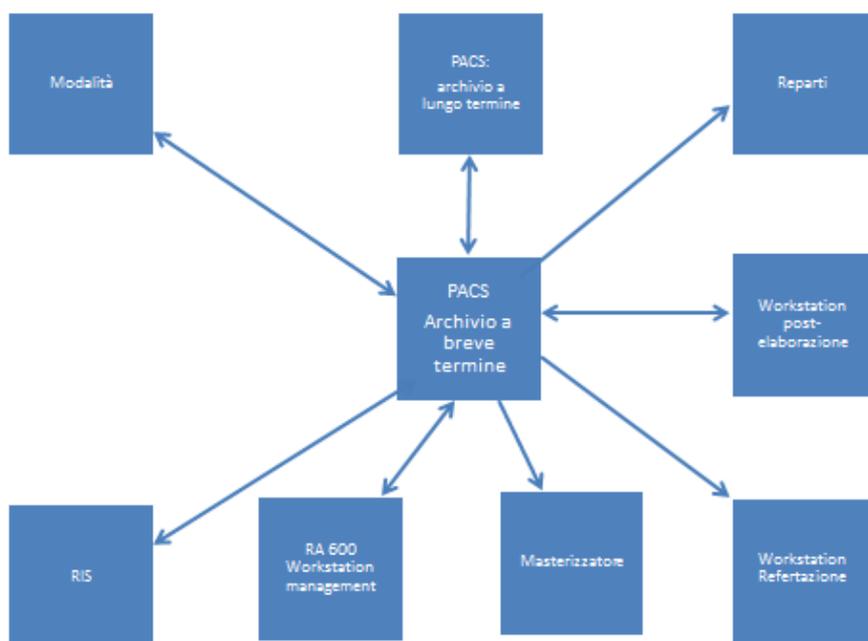


Fig.3 Illustrazione del PACS

La struttura del PACS dell'AOU Ospedali Riuniti di Ancona conta 87 dispositivi, tra workstation dedicate alla refertazione, workstation dedicate alla post-elaborazione e client server del RIS.

Tali dispositivi si articolano nel seguente modo: 78 di loro hanno come sistema operativo Windows XP professional, 6 di loro hanno Windows 2000 professional, ed infine 3 di loro presentano come sistema operativo Microsoft Windows NT.

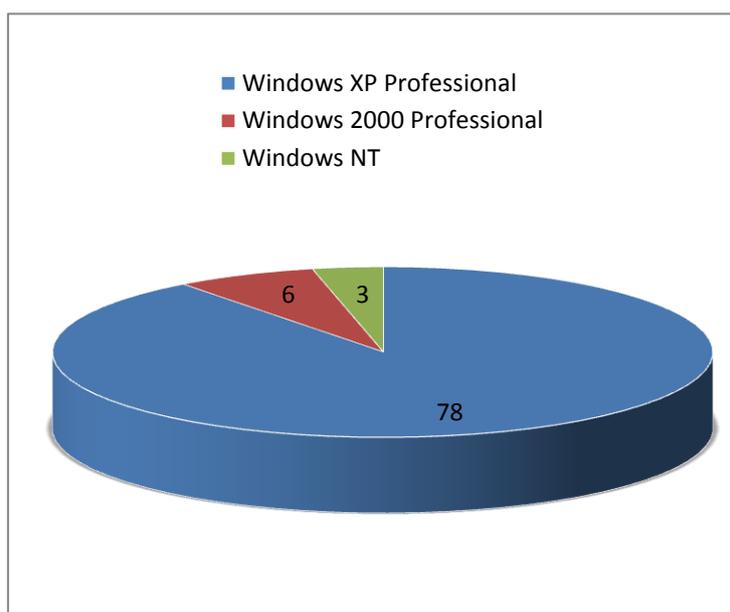


Fig.4 Sistemi operativi presenti nei computer collegati al PACS.

1.6 Modalità diagnostiche

Le modalità diagnostiche sono rappresentate dalla tomografia computerizzata, dalla risonanza magnetica, e dalla radiologia digitale, dalla medicina nucleare, dall'angiografia digitale, dall'ecografia ad ultrasuoni e dalla mammografia.

Il collegamento tra PACS e modalità avviene per mezzo dei computer di acquisizione, i quali dopo aver acquisito le immagini dalle varie modalità, le convertono in formato DICOM e le trasferiscono al PACS.

I computer di acquisizione e le varie modalità diagnostiche sono collegati tramite rete ethernet, con protocolli TCP/IP.

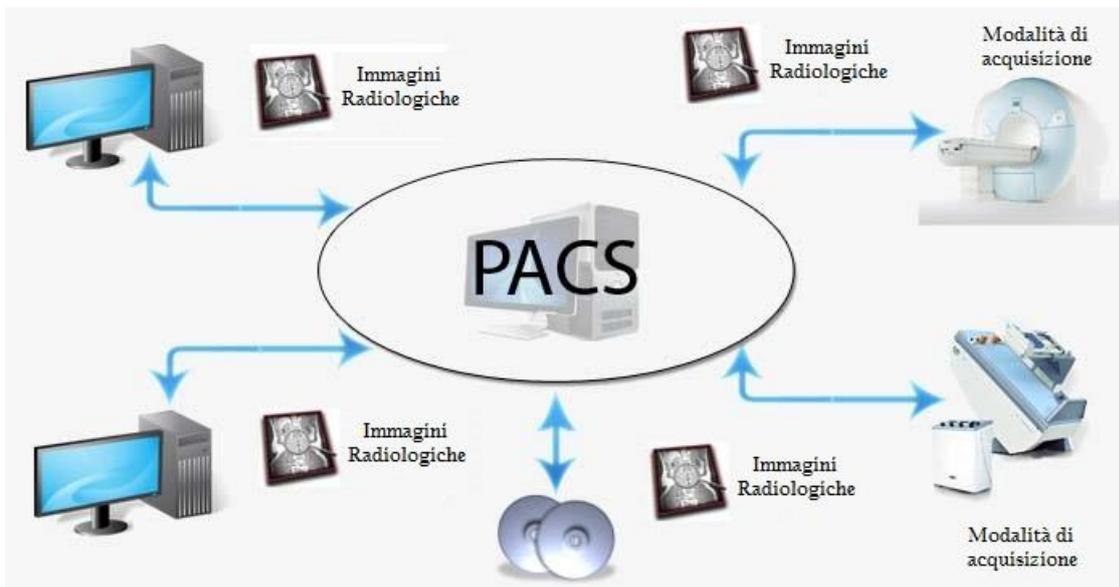


Fig.5 Flusso delle immagini nel sistema PACS.

Sistemi PACS - Modalità

Modalità	Sigla
Computed Radiography	CR
Digital Radiography	DR
Computed Tomography	CT
Magnetic Resonance	MR
Nuclear Medicine	NM
Ultrasound	US
Positron Emission Tomography (PET)	PT
Mammography	MG
X-Ray Angiography	XA
Radio Fluoroscopy	RF
Endoscopy	ES
Other	OT

Fig.6 Elenco delle modalità diagnostiche integrate su PACS aziendale

Al sistema PACS dell'Azienda Ospedaliera Ospedali Riuniti di Ancona, sono collegati 7 apparecchiature TC, 20 apparecchiature che producono immagini di radiologia convenzionale, di cui 8 portatili, 6 angiografi, di cui 4 digitali, di questi 1 monoplanare ed 1 biplanare, 3 mammografi digitali.

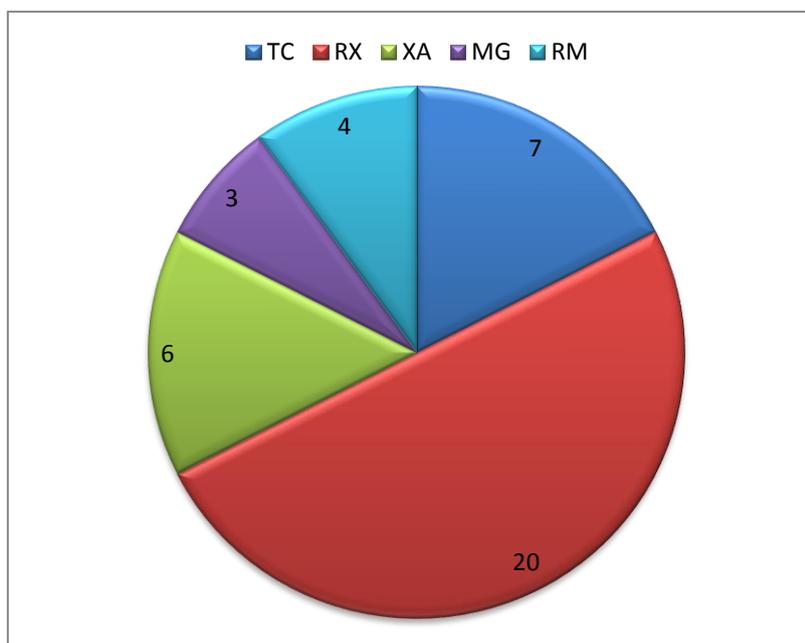


Fig.7 Modalità diagnostiche collegate al PACS dell'Ospedale Riuniti di Ancona.

1.7 Workstation

In radiologia, è possibile utilizzare postazioni di lavoro al fine di refertare l'immagine diagnostica, precedentemente acquisita; oppure eseguire post-processing, al fine di facilitare la refertazione al medico radiologo.

Le Workstation, che siano quelle dedicata alla refertazione, o che siano quelle dedicate al post-processing, si interfacciano col sistema PACS, tramite standard DICOM.

DICOM File Format si occupa di definire come devono essere incapsulate le immagini, in un file completo dal punto di vista medico; esso permette di includere il referto all'interno del file, contenente anche le immagini.

Negli Ospedali Riuniti di Ancona sono presenti 17 Workstation dedicate alla refertazione, e 18 Workstation dedicate al post processing, come mostrato dal grafico sottostante.

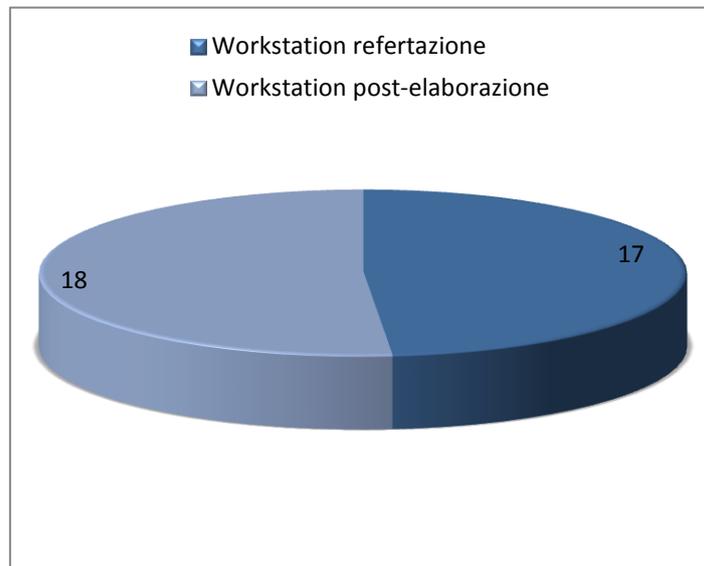


Fig.8 Workstation AOU

Le workstation dedicate alla refertazione sono ubicate in entrambi i poli ospedalieri, quello di Torrette e quello dell'Ospedale Materno Infantile Salesi.

Nel polo di Torrette sono suddivise così:

- nella sala referti della neuroradiologia,
- nella sala referti ospedaliera,
- nella sala referti della TC del pronto soccorso,
- nella sala referti clinica.

Al Salesi sono :

- nella sala refertazione TC,
- nella sala refertazione RM,
- nella sala referti 1,
- nella sala referti 2,
- nella sala riunioni.

Naturalmente i due poli sono strettamente connessi, le WS hanno indirizzi IP diversi perché sono collocate in reti separate fisicamente all'interno della stessa città, ma comunque affluiscono allo stesso sistema PACS e di conseguenza sugli stessi sistemi aziendali.

Capitolo 2 : Aggiornamento del PACS

L'ambiente informatico è in continua evoluzione, ed alcune apparecchiature dopo anni dalla loro installazione non sono più manutenibili.

Inoltre con l'installazione di nuove modalità ed il conseguente aumento dei volumi di esami, si è visto necessario adeguare le dimensioni dei dispositivi di archiviazione e potenziare anche Workstation e Server PACS.

2.1 Obiettivi

Con l'aggiornamento del PACS, si mira a :

- Garantire la continuità di funzionamento ed il livello prestazionale dell'intero sistema PACS in uso presso il dipartimento di scienze radiologiche.
- Preservare la sicurezza dei dati su sistemi client e server.
- Rispondere in modo efficiente alle sempre maggiori esigenze cliniche ed alle nuove tecnologie TC presenti in ospedale.
- Adeguare alle esigenze delle nuove tecnologie i sistemi di archiviazione a lungo termine ed a breve termine, in termini di capacità degli storage.

Altro obiettivo chiave è garantire una continuità del funzionamento del sistema anche in caso di "failure", e ciò presuppone la ricerca di una migliore soluzione hardware e software.

2.2 Innovazioni

In seguito, vengono elencate le principali novità relative all'aggiornamento del PACS.

- Aggiornamento del sistema per le componenti Hardware server e storage al fine di supportare le ultime versioni dei sistemi operativi.
- La componente software Enterprise Archive, adibita alla gestione dell'archivio a lungo termine, sarà aggiornata all'ultima versione disponibile.
- La componente Software Centricity Web, ossia lo strumento di visualizzazione delle immagini PACS nei reparti, sarà aggiornata con il sistema Centricity Zero Foot Print.
- Aggiornamento e sostituzione del software RA100 con il software Centricity Universal Viewer, compatibile con Windows 10.
Centricity PACS con Universal Viewer è un sistema medicale di classe II che permette la consultazione e refertazione delle immagini radiologiche diagnostiche.
- Sostituzione delle workstation, con workstation di ultima generazione con sistema operativo Windows 10.
- Introduzione di Centricity RA600, stazione di lavoro completamente DICOM, ideale per la refertazione primaria o la visualizzazione secondaria degli esami radiologici.
In caso di guasto, rende comunque possibile la visualizzazione delle immagini, nonostante il temporaneo inutilizzo del sistema PACS.
- Sostituzione di una parte dei monitor diagnostici attualmente installati, risultanti obsoleti in termini di ore lavorate o anni di produzione.

Leggenda :

Versione precedente
 Aggiornamento



Fig.9 Come cambia il PACS dopo l'aggiornamento : in rosso vengono evidenziate le componenti che cambiano rispetto la versione precedente.

2.3 Architettura tecnica

L'attuale sistema PACS prevede l'utilizzo di una infrastruttura fisica, in cui, ad ogni funzione corrisponde un server.

Ciò implica che se un server si guasta, la funzione svolta da tale server diventa indisponibile.

Inoltre tale architettura presuppone un alto consumo di spazio nel datacenter, un alto consumo di energia elettrica, ed un'alta produzione di calore.

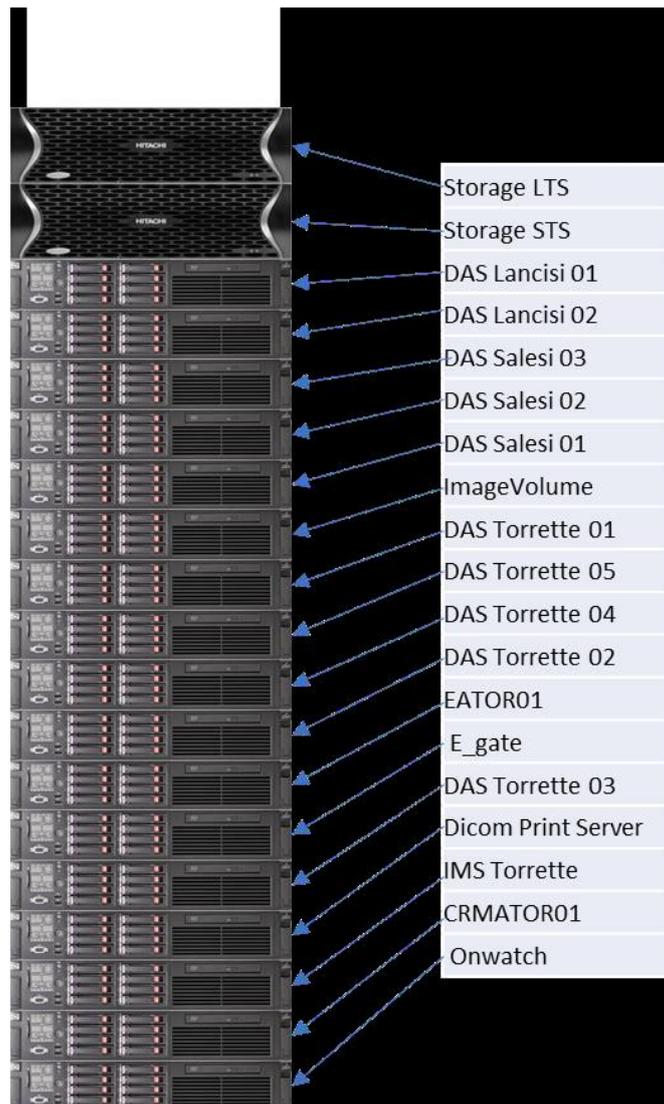


Fig.10 Configurazione attuale dei server PACS.

La nuova soluzione prevede la virtualizzazione della infrastruttura, la quale permette di consolidare i server ed aumentare l'indice di fragilità, ossia la capacità di riorganizzarsi dopo eventi avversi.

Con l'aggiornamento il sistema PACS baserà il suo funzionamento su un hardware Dell VRTX, che dispone di potenza di calcolo, connettività e storage completamente integrati ed ottimizzati.

La presenza di server blade minimizza l'occupazione dello spazio e riduce al minimo la formazione di eventuali colli di bottiglia, frequenti quando vengono adottate soluzioni server con storage esterno.

Inoltre lo spazio occupato nel datacenter, si riduce a poche unità, come anche lo storage ad altissima densità.

Una seconda copia dello storage può essere collocata in un altro presidio o nel cloud.

Se uno dei server blade all'interno del VRTX dovesse guastarsi, i servizi che questo stava eseguendo, saranno presi in carico dalle lame restanti consentendo in pochi minuti di rendere nuovamente disponibile il sistema nella sua totalità.

Da quanto citato, si ottiene:

- Riduzione dei tempi di ripristino in caso di guasto
- Riduzione dello spazio fisico
- Riduzione del consumo di energia elettrica
- Riduzione della produzione di calore

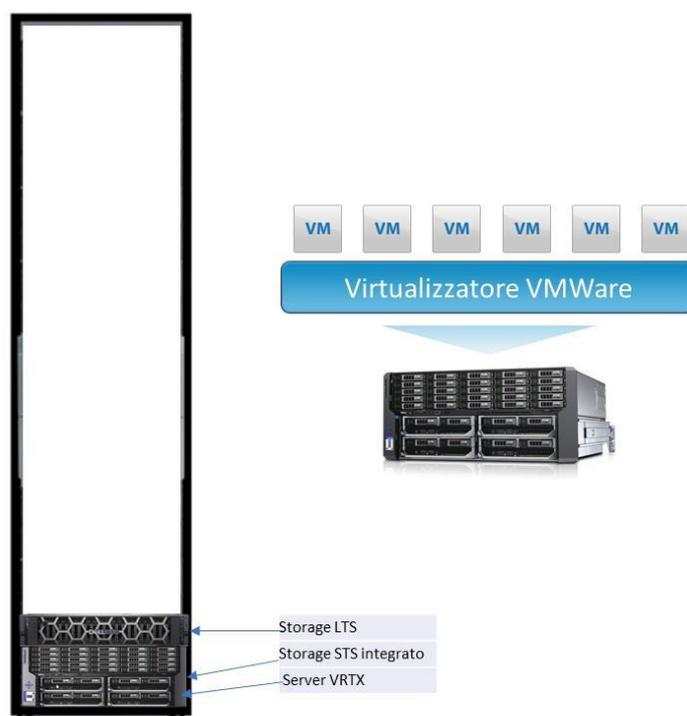


Fig.11 Nuova architettura sistema PACS

La nuova architettura comprende :

- Soluzione base con alta affidabilità grazie al cluster VMWare
- Archivio di breve termine integrato da 16 TB netti ca. (pari a 3 anni ca.)
- Archivio di lungo termine esterno da 100 TB netti ca. (storico + nuova produzione per 3 anni)

2.4 Centricity Clinical Archive (Enterprise Archive)

Il sistema Centricity Clinical Archive è adibito alla gestione dell'archiviazione a lungo termine delle immagini e dei referti.

Il sistema di archivio verrà reso compatibile con i sistemi operativi più recenti tramite l'aggiornamento all'ultima versione.

Con quest'ultimo aggiornamento, si estendono le funzionalità di archiviazione delle immagini DICOM, rendendo l'archivio centralizzato e multidisciplinare, in grado di trasformare gli archivi dipartimentali in potenti strumenti di condivisione delle informazioni.

2.5 Centricity Zero Foot Print

Come precedentemente accennato, con l'aggiornamento del PACS la componente Software Centricity Web sarà aggiornata con il sistema Centricity Zero Foot Print.

Quest'ultimo permette la distribuzione ai reparti di immagini e referti via web, secondo gli standard di sicurezza, e rispettando a pieno le normative sulla privacy.

Il concetto attorno al quale ruota l'utilizzo di questo sistema Centricity Zero Foot Print è quello di poter permettere l'accesso a qualsiasi informazione sempre ed ovunque.

Sarà possibile raggiungere tali informazioni, semplicemente anche tramite smartphone cosicché i reparti potranno raggiungere tali informazioni velocemente mediante link su portale intranet.

La distribuzione ai reparti è possibile non appena gli esami vengono archiviati in Enterprise Archive e l'elenco degli studi può essere visualizzato tramite un semplice browser, confermando dunque la possibilità di un accesso rapido e semplice alle informazioni sui pazienti ed a studi vitali archiviati nel sistema PACS.

Non è infatti richiesta nessuna installazione di componenti aggiuntive per adempiere a tali obiettivi.

Tutti i medici referenti possono disporre delle stesse funzionalità avanzate di post-elaborazione del radiologo, così da poter consultare un ampio set di dati direttamente dal proprio ambulatorio, mediante un'applicazione desktop.

L'accesso alle immagini archiviate e refertate è basato su diversi livelli di autorizzazione e livelli di sicurezza basati su profili utente.

L'architettura di Centricity PACS si basa sull'accesso On Demand Cacheless (cioè senza richiedere il pre-caricamento delle immagini da consultare sui dischi locali) alle informazioni (dati ed immagini), da soluzioni di archiviazione ad elevata sicurezza (accesso sicuro tramite protocollo https) ed alta velocità di accesso ai dati (SAN, NAS).

Poiché il sistema è cacheless, i reparti accedono in tempo reale alla stessa immagine visualizzata dalle radiologie, così da garantire la consistenza e la correttezza del dato visualizzato.

Le immagini potranno essere disponibili per i reparti, a seconda della configurazione, in determinati stati del processo: eseguito, refertato, firmato. In base alle esigenze dei processi interni, le immagini potranno pertanto essere rese disponibili solo dopo la refertazione o dopo l'esecuzione. Il Sistema potrà inviare la notifica HL7 al repository segnalando la disponibilità delle immagini per la visualizzazione.

In definitiva i radiologi ed i clinici hanno facoltà di :

- Accedere alla storia di imaging del paziente tramite browser web e senza l'utilizzo di plug-in
- Visualizzare referti ed immagini chiave con la possibilità di utilizzare gli strumenti di post processing (MIP,VR,... ecc)
- Visualizzare altri contenuti clinici in molteplici formati
- Effettuare un confronto tra più identificativi del paziente
- Utilizzare lo stesso sistema PACS



Fig.12 Centricity Zero Foot Print

2.6 Centricity Universal Viewer

Centricity PACS con Universal Viewer è un sistema medicale di classe II sviluppato per soddisfare le esigenze del personale medico nella consultazione e refertazione delle immagini radiologiche diagnostiche.

Esso basa il suo funzionamento tramite l'utilizzo di un visualizzatore sviluppato su tecnologia web, il quale permette di lavorare in modo sincrono ed unificato a radiologici e clinici.

La workstation è munita di tutte le applicazioni necessarie per svolgere il post-processing, eliminando la necessità di spostarsi su un'altra postazione.

Sono limitate al minimo le richieste di nuovo invio DICOM e di spostamento delle immagini tra le varie modalità diagnostiche.

Universal Viewer permette, inoltre, la personalizzazione, affinché ogni utente possa adattare il sistema alle esigenze del proprio workflow.

L'interfaccia che l'utente sceglie, viene riproposta indipendentemente dalla postazione dalla quale si accede al server PACS.

Il sistema Centricity PACS permette la selezione degli esami e dei pazienti mediante parametri multipli di interrogazione (per nome, per data, per descrizione, per ID paziente, per parola chiave, ecc.).

Inoltre è possibile creare gruppi di lavoro ed accesso virtuali, volti a favorire consulenze esterne.

Il software permette anche di poter scegliere la modalità di visualizzazione, tra "lights on" e "lights off", al fine di garantire il comfort di lettura in qualsiasi condizione luminosa.

In base all'algoritmo "Pixel on Demand", per quanto concerne la visualizzazione delle immagini sul monitor, il sistema è in grado di riconoscere la definizione del monitor, ed invia solo il dettaglio visualizzabile da quest'ultimo; ottimizzando al meglio il flusso di informazioni.

La tecnologia SmartLoading permette l'analisi del formato di archiviazione delle immagini (JPEG, JPEG2000, RLE) e le condizioni della connessione di rete tra

il visualizzatore e l'archivio, in modo da individuare il modo più efficiente per la visualizzazione delle immagini.

La prima immagine inviata, viene visualizzata dopo appena 2 secondi, inoltre la qualità dell'immagine si adatta all'istante alla risoluzione del monitor utilizzato.

All'interno dello stesso monitor, o su monitor differenti, è possibile anche confrontare più studi, ciò risulta funzionale se ad esempio si vogliono confrontare due TC cerebrale dello stesso paziente, oppure una TC ed una RM del medesimo distretto anatomico dello stesso paziente.

L'utente può decidere se visualizzare le informazioni reputate non essenziali, definendole appunto le informazioni di overlay.

L'utente può inserire nel PACS commenti testuali collegati allo studio DICOM.

E' possibile esportare e salvare immagini in diversi formati, tra cui bmp, jpg, tif.

Il sistema supporta il formato DICOM JPEG/JPEG 2000 lossless e lossy, ed è in grado di variare parametricamente il livello di compressione (tipo lossless o lossy).

Infine, è possibile produrre localmente sulle workstation i CD Patient delle immagini desiderate ed importare da CD/DVD standard DICOM.

Centricity PACS dunque esprime le sue finalità mediante:

- Applicazioni di visualizzazione avanzate con Advantage Windows Server, in cui alle funzionalità di visualizzazione native, vengono aggiunti gli strumenti di post-elaborazione 3D, sia in ambito radiologico che cardiologico.

E' possibile, eseguire MIP/MPR, analisi vasale, rimozione automatica delle ossa, fusione e registrazione per più modalità e ricostruzioni 3D e 4D delle strutture cardiache.

Ciò evita che l'utente debba accedere a più sistemi per recuperare le immagini necessarie, eliminando così le richieste di rinvio DICOM.

- Strumenti intelligenti per migliorare la produttività.

Si riducono sensibilmente le tempistiche di configurazione degli esami.

“ Smart Reading Protocols “ valuta i dati e suggerisce il metodo più appropriato di uno studio in base alle preferenze del singolo utente.

- Possibilità di accedere ovunque per effettuare la revisione clinica.
- Unica lista di lavoro di tutti gli esami prodotti dall'intera azienda, che favorisce la condivisione del flusso di lavoro tra le sedi.
- Elevate prestazioni del sistema grazie alla tecnologia Streaming in grado di adattarsi alla larghezza di banda.

Sono così ottimizzate le prestazioni in ambienti con connessione di rete lente, l'utente però ha la possibilità di iniziare l'attività di post-processing prima che tutto il set di immagini sia stato trasferito.

E' dunque possibile, lavorare da remoto in consultazione o in second opinion.

Universal Viewer permette, relativamente a visualizzazione, presentazione e processing delle immagini :

- di adattare tali immagini al display di visualizzazione (auto-scale),
- di accoppiare simmetricamente ed allineare le immagini (auto-align),
- di far comparire i dati acquisiti rapidamente (auto-update),
- di mostrare una galleria di miniature, la quale dà una panoramica di tutte le immagini disponibili per un paziente (image folder),
- di ordinare le immagini secondo ordine cronologico ed allinearle secondo l'asse orizzontale,
- di raggruppare secondo l'asse verticale le immagini per tipologia,
- di poter ingrandire e confrontare mediante allineamento una coppia di immagine,
- di cambiare l'orientamento di un'immagine, tramite inversione, rotazione o capovolgimento,
- di annotare testi come DICOM presentation state.

Permette inoltre numerose opzioni di zoom, tra cui la visualizzazione panoramica, la visualizzazione in formato originale, l'auto scale, lo zoom libero continuo, il quadrant zoom e il navigator zoom.

L'utente può agire anche su contrasto e luminosità, usando il mouse è possibile apportare correzioni per un'unica immagine, per un gruppo di esse o per tutte.



Fig.13 Centricity Universal Viewer

2.7 Centricity SenoIris Workstation

Centricity Senoris permette un'approfondita comprensione clinica del percorso mammografico, supportando i flussi di lavoro di screening e diagnostici, e la visualizzazione d'immagini multimodali.

Viene così eliminata la necessità di leggere le immagini mammografiche su workstation diverse.

Senolris è progettata per visualizzare immagini mammografiche digitali dirette (DR) e radiografie computerizzate (CR), oltre che altre modalità di imaging del seno, come l'ecografia e la risonanza magnetica.

Inoltre è supportata la lettura di immagini di tomosintesi e di Contrast Enhanced Spectral Mammography (CESM).

Mediante un algoritmo di elaborazione, è possibile aumentare la visibilità delle strutture della mammella, ed equalizzare lo spessore dell'immagine per migliorare la visibilità dei tessuti sottocutanei.



Fig.14 Centricity Senolris Workstation

2.8 Workstation di refertazione

Con l'aggiornamento del sistema PACS si provvede alla sostituzione di n.30 workstation di radiologia e n.4 workstation di senologia.

Tali workstation saranno compatibili con Windows 10, portando benefici in termini di prestazioni e sicurezza.

In radiologia è prevista la fornitura di postazioni Dell Precision 5820 Tower con 1 Intel Xeon W-2145 (3.7 GHz, 4.5 GHz Turbo, 8C, 11 MB Cache, HT (140W)) DDR4-2666, RAM 16 GB, Sistema Operativo Windows 10, comprensive di monitor Dell 22".

In senologia è prevista la fornitura di postazioni Dell Precision 7820 Tower con 2 Intel Xeon Bronze 3106 1.7 GHz, 8C, 9.6 GT/s 2UPI, 11MB Cache, No turbo, No HT (85W) DDR4-2133 2nd, RAM 32 GB, Sistema Operativo Windows 10, comprensive di monitor Dell 22".



Fig.15 Workstation di refertazione

2.9 Monitor Diagnostici

Dopo aver effettuato una analisi condotta sui monitor diagnostici, relativa all'obsolescenza, si opta per la sostituzione, tenendo conto delle ore lavorate (40000h) e dell'anno di produzione (<2005).

Sono stati perciò sostituiti, a causa delle eccessive ore di lavoro :

- N.6 Monitor da 2 Megapixel
- N.6 Monitor da 3 Megapixel
- N.6 Monitor da 5 Megapixel

E sono stati sostituiti, a causa dell'anno di produzione :

- N.2 Monitor da 2 Megapixel
- N.4 Monitor da 3 Megapixel
- N.2 Monitor da 5 Megapixel

I monitor diagnostici presentano le seguenti caratteristiche :

- Monitor 2MP: ECR-DG-2MC con Luminosità Massima: 800 cd/m²
- Monitor 3MP: ECR-DG-3MC con Luminosità Massima: 1000 cd/m²
- Monitor 5MP: EIZO RadiForce GX560 con Luminosità Massima: 2.500 cd/m²

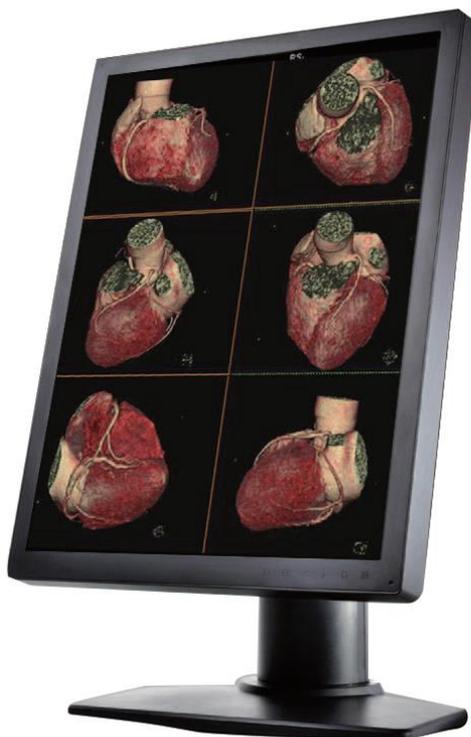


Fig.16 Monitor diagnostico 3 Megapixel

2.10 Centricity RA600

Centricity RA 600 è una stazione di lavoro completamente DICOM, utile ai fini della refertazione prima o della visualizzazione secondaria degli esami radiologici.

Con l'installazione di N.3 sistemi Centricity RA600, di cui uno in modalità software only, si assolve il problema della gestione di eventuali guasti del sistema PACS, che impedivano l'immediata visualizzazione delle immagini.

Ad eccezione del sistema Centricity RA600 installato in modalità software only, gli altri due comprendono workstation complete di hardware a monitor diagnostici da 3MP.

Le RA600 possono essere configurate come dei nodi DICOM stand alone, ossia in maniera indipendente dalle altre unità di elaborazione.

Ciò consente di configurare un ulteriore nodo di invio manuale delle immagini DICOM, da sfruttare in caso di guasto del PACS.

Le immagini così potranno essere inviate e visualizzate direttamente sulla RA600, e se necessario potranno essere masterizzate su CD/DVD direttamente sulla workstation.



Fig.17 Centricity RA600

Capitolo 3 : Cenni di sicurezza informatica

La crescente interconnessione dei dispositivi medici e l'uso di connessioni remote per la loro manutenzione; la necessità di monitorare continuamente i pazienti - anche quelli fuori dall'ospedale; l'uso di smartphone per accedere alle informazioni sanitarie da parte di pazienti e medici, insieme alle difficoltà nel mantenere aggiornati i sistemi sia HW che SW legate alla non proporzionalità alle esigenze di cybersecurity rispetto alle risorse economiche destinate, rendono il settore sanitario particolarmente vulnerabile.

Considerazioni circa la sicurezza informatica dovrebbero essere fatte prima di qualsiasi acquisto di infrastrutture, software, sistemi, dispositivi, ecc.

3.1 Legislazione europea ed internazionale

La legislazione ha un ruolo chiave nella definizione dei requisiti di sicurezza informatica che dovrebbero essere definiti nelle specifiche tecniche quando si ottengono prodotti e servizi in un ospedale.

In campo europeo le leggi/direttive più importanti sono:

- **La direttiva sulla sicurezza delle reti e dell'informazione (NISD):** entrata in vigore nel mese di maggio del 2018, si pone come obiettivi l'attuazione di requisiti minimi di sicurezza, e l'istituzione di notifiche di sicurezza informatica per gli operatori ed i fornitori di servizi essenziali. Gli ospedali sono considerati fornitori di servizi essenziali. La direttiva, inoltre, conferisce agli enti regolatori, facoltà di controllo ad operatori dei servizi essenziali, affinché il livello di sicurezza informatica nell'organizzazione sia accettabile e conforme alle disposizioni della direttiva.

- **Regolazione dei dispositivi medici (MDR):** si tratta di un regolamento che dispone specifiche relative alla sicurezza informatica per tutti i dispositivi medici.

Ripetibilità, affidabilità e prestazioni secondo l'uso previsto fanno parte dei requisiti generali di sicurezza e di prestazioni definiti nel MDR.

Il Medical Device Coordination Group (MDCG), nel dicembre 2019, ha pubblicato "Guidance on Cybersecurity for medical devices" al fine di fornire una guida su come soddisfare i requisiti essenziali contenuti nel MDR.

L'MDCG è composto da rappresentanti di tutti gli Stati membri ed è presieduto da un rappresentante della Commissione Europea.

L'MDCG fornisce consulenza alla Commissione e assiste la Commissione e gli Stati membri nell'attuazione dei regolamenti sui dispositivi medici.

- **Regolamento generale sulla protezione dei dati (GDPR):** entrato in vigore il 25 maggio 2018, stabilisce le norme per il trattamento e la libera diffusione dei dati personali.

Tale regolamento si applica sia al settore pubblico, che al settore privato; sebbene vi sono alcune deroghe specifiche riguardanti i dati relativi alla salute.

Tali deroghe mirano alla tutela dei diritti delle persone interessate, ed alla riservatezza dei loro dati personali circa la salute; ma puntano anche a preservare il trattamento dei dati personali ai fini della ricerca e della salute pubblica.

Dunque, secondo il GDPR i dati sanitari sono una categoria speciale di dati personali, perciò vi si impone uno standard di protezione più elevato per il loro trattamento.

Per trattare dati sanitari, bisogna adempiere all'attuazione di misure tecniche ed organizzative, tali da garantire la sicurezza dei sistemi di trattamento dei servizi e dei dati personali.

Occorre inoltre effettuare una valutazione d'impatto sulla protezione dei dati, e segnalare entro 72 ore dal momento in cui se ne viene a

conoscenza, eventuali violazioni dei dati, tali da comportare un rischio per la privacy dell'individuo.

La violazione dei dati personali, definita all'articolo 4 del GDPR, è una violazione della sicurezza che comporta la distruzione accidentale o illecita, la perdita, l'alterazione, la divulgazione non autorizzata, o l'accesso ai dati personali trattati.

- **Guida FDA per la sicurezza informatica**

Sviluppata dalla FDA, individua gli aspetti fondamentali relativi alla sicurezza informatica che i produttori dovrebbero tenere in considerazione durante la progettazione e lo sviluppo dei dispositivi medici.

Se un produttore punta al mercato interno, il dispositivo deve essere conforme alla legislazione europea ed internazionale.

3.2 La sicurezza informatica all'interno del processo di approvvigionamento

Poiché l'ecosistema ospedaliero è composto da diversi componenti informatici, la sicurezza informatica dovrebbe essere esaminata separatamente in tutti questi diversi componenti.

La sicurezza informatica dovrebbe far parte di tutte le diverse fasi del processo di approvvigionamento.

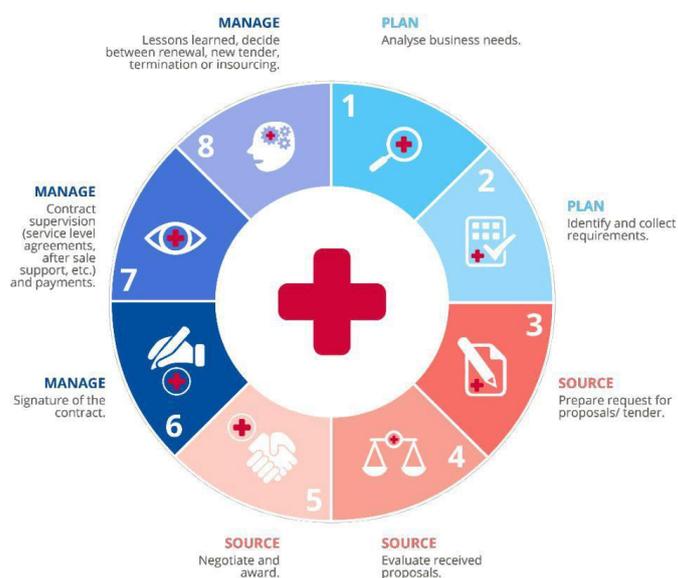


Fig.18 Ciclo di vita del processo di approvvigionamento per gli ospedali

Durante la fase di pianificazione l'ospedale, in base alle esigenze interne, raccoglie le richieste dei vari reparti.

In questa fase, si stabiliscono i requisiti specifici di sicurezza informatica per i nuovi approvvigionamenti.

Nella fase di "sourcing", i requisiti vengono tradotti in specifiche tecniche, e viene dunque pubblicata una gara d'appalto in cui l'ospedale riceve e valuta le offerte designate, selezionando i prodotti più appropriati.

Alla fine delle trattative con l'appaltatore, si stipula un contratto.

In questa fase, all'interno del contratto vengono inserite le caratteristiche di sicurezza dei prodotti e le responsabilità dei fornitori per gli aspetti di sicurezza informatica.

Durante la fase della gestione e del monitoraggio, il contratto viene assegnato all'imprenditore, e si chiude la gara d'appalto.

Da qui si monitorano continuamente gli aspetti della sicurezza informatica, quali incidenti e nuove vulnerabilità e vengono applicate eventuali misure correttive, quali le "patch", utili al mantenimento di un elevato livello di sicurezza.

Quando i prodotti verranno messi in disuso, per motivi di privacy, sarà necessario uno smaltimento sicuro, in quanto i dispositivi dispongono di informazioni sui pazienti.

3.3 Standard e linee guida di settore rilevanti

Esistono una serie di regolamenti, standard internazionali e buone pratiche sui sistemi sanitari, nella quale sono incluse nozioni di base della sicurezza informatica.

Ad esempio la dichiarazione informativa del produttore per la sicurezza dei dispositivi medici (MDS2), fornisce ai produttori dei dispositivi medici un mezzo per divulgare le caratteristiche di sicurezza dei loro dispositivi medici.

Tramite una serie di domande sulla sicurezza di tali dispositivi, contenuti nei moduli, è consentito confrontare le caratteristiche di sicurezza dei vari dispositivi e dei molteplici produttori.

L'Organizzazione internazionale per la normazione (ISO), ossia la più importante organizzazione a livello mondiale per la definizione di norme tecniche, sta sviluppando nuovi standard relativi all'informatica medica, tra cui :

- *ISO/DTR 22696* Informatica sanitaria - Guida all'identificazione e all'autenticazione dei dispositivi sanitari personali collegabili
- *ISO/DTR 21332* Informatica sanitaria - Considerazioni sul cloud computing per la sicurezza e la privacy dei sistemi informativi sanitari

- *ISO/WD 13131* Informatica sanitaria - Servizi -Linee guida per la pianificazione della qualità
- *ISO/AWI 22697* Informatica sanitaria - Applicazione della gestione della privacy alle informazioni sanitarie personali

Inoltre, come mostrato nella figura sottostante, nella UE e negli Stati membri esistono una serie di linee guida e di standard.



Fig.19 Linee guida e standard europei

3.4 Tassonomia delle minacce

Nel processo di analisi del rischio, occorre considerare le molteplici fonti di minaccia, che vanno a sfruttare le vulnerabilità del sistema.

Esempi di fonti di minaccia sono: un hacker, il guasto di un dispositivo di memorizzazione, il guasto di un sistema operativo, un incendio, ecc.

Le minacce possono essere suddivisi in 5 gruppi principali :

- fenomeni naturali,
- guasto della catena di fornitura,
- errori umani,
- azioni malevole,
- guasti del sistema.

Per **fenomeni naturali**, si intendono incendi, inondazioni e terremoti, sebbene siano eventi rari.

In caso di tali eventi, i macchinari più colpiti sono le TC, le apparecchiature RM, e gli acceleratori lineari per la radioterapia.

Un eventuale **guasto della catena di fornitura**, potrebbe colpire ad esempio il fornitore dei servizi di cloud.

Un eventuale guasto nel cloud, se non supportato per funzionare off-line potrebbe causare interruzioni nella fornitura di servizi medici.

Per evitare che un guasto del provider di rete possa avere ripercussioni, si punta sulla ridondanza dell'architettura dei sistemi informatici.

Inoltre, se si acquista un dispositivo fuori dal mercato, potrebbero verificarsi problemi con gli aggiornamenti del dispositivo, e tale problematica è difficilmente risolvibile.

Per quanto riguarda gli **errori umani**, vanno considerati ad esempio errori di configurazione del sistema medico, tra cui la mancata modifica delle password di fabbrica, o la configurazione del dispositivo che consente le connessioni in ingresso da qualsiasi indirizzo, o ancora la comunicazione tramite protocolli non criptati.

Un altro errore umano, è quello di non conservare o compilare i registri di audit, poiché tali registri, sono uno strumento fondamentale per risalire (tramite i log) a come eventuali aggressori siano entrati all'interno del sistema.

Si possono così valutare anche quante informazioni vengono compromesse.

Alcune politiche aziendali permettono di portare i propri dispositivi personali nel posto di lavoro ed utilizzarli per avere gli accessi privilegiati alle informazioni aziendali e alle loro applicazioni.

Questa politica, chiamata BYOD (bring your own device), può rappresentare un rischio significativo per le organizzazioni, poiché se i dispositivi non vengono abilitati in modo sicuro, sono esposti ad attacchi malware ed a furti di dati personali.

Va inoltre considerata l'eventualità di un errore umano durante l'inserimento dei dati, come ad esempio lo scambio di informazioni cliniche tra due pazienti omonimi.

Tale evento potrebbe avere un impatto rilevante sulla reputazione dell'azienda.

I malware sono l'esempio più rappresentativo per ciò che si intende come **azione malevole**, volta a danneggiare il sistema.

I malware sono favoriti dalle interconnessioni presenti nei sistemi IT.

Il vettore con cui si diffondono più facilmente i malware sono gli adware.

Un esempio di malware, è il ransomware, il quale limita l'accesso del dispositivo infettato richiedendo un riscatto da pagare per rimuovere la limitazione.

Come precedentemente accennato, le imprese che consentono l'utilizzo del proprio dispositivo senza polizze adeguate, sono esposte a rischi aggiuntivi.

Altro vettore che favorisce le infezioni da malware è la posta elettronica.

La maggior parte delle organizzazioni consente ancora l'accesso ad account web privati di posta elettronica nella maggior parte dei computer dell'ospedale.

Gli indirizzi postali dei medici sono facili da raccogliere attraverso gli elenchi pubblici degli ospedali, le presentazioni esistenti sul web, ecc.

Altra problematica da tenere in considerazione sono le comunicazioni non protette tra i dispositivi medici ed i server, le quali possono portare alla manomissione delle informazioni.

Attacchi "man in the middle" possono modificare i dati provenienti ad esempio dalle immagini DICOM provenienti dalle TC, RM nel loro percorso verso il server PACS.

Un'altra tipologia di cyberattacco è la negazione del servizio, la quale abbatte i server di un'organizzazione sanitaria, spesso perché queste ultime non utilizzano l'infrastruttura cloud pubblica.

Altro rischio per i sistemi informatici è la gestione di tali da parte di personale non autorizzato o scarsamente addestrato, con il rischio di manipolazione, danneggiamento, furto o perdita dei beni informativi contenuti.

Un'altra azione malevole che coinvolge il personale sanitario è il furto di identità, che può provocare la diagnosi di una malattia ad un paziente in realtà sano.

Tra i problemi che possono essere causati dal sistema, vanno considerati i **guasti del software**: i server sono più soggetti, soprattutto perché si affidano ad altre piattaforme software (sistemi operativi, framework di programmazione, database) che possono fallire.

I guasti nei server medici si verificano normalmente come errori latenti e, in alcune occasioni, possono interrompere il servizio, essi scompaiono abitualmente dopo il riavvio del server.

L'analisi dei log generati è fondamentale per individuare la causa dell'errore.

I guasti che invece non causano malfunzionamento al server o al servizio in sé, vengono solitamente rilevati mesi dopo che il sistema è stato riavviato.

È molto difficile eseguire test per garantire che il sistema funzioni correttamente, poiché spesso tali sistemi lavorano 7 giorni su 7, per tutto il giorno.

È inoltre fondamentale aggiornare i firmware in tutti i dispositivi dell'ospedale perché i dati sanitari sensibili potrebbero essere esposti a pericoli.

È fondamentale che l'ecosistema di un ospedale sia resiliente, affinché il guasto di un componente, non provochi effetti a cascata su altri sistemi sanitari.

Ultimo problema da considerare circa eventuali guasti nel sistema, è la manutenzione insufficiente, poiché la mancanza di patch può favorire la diffusione di malware, esponendo i dati sensibili dei pazienti.

3.5 Valutazione critica e applicazione del documento

Gli obiettivi principali della sicurezza informatica dei sistemi medicali possono riassumersi nella capacità di preservare ed evitare qualsiasi danneggiamento HW e SW, e soprattutto nel garantire la sicurezza e riservatezza dei dati interni al sistema, evitando così la perdita di dati sensibili.

Al fine di garantire la sicurezza informatica di un sistema è stato stilato un documento al cui interno, divisi rispettivamente per argomenti, vi sono gli aspetti principali da conoscere di un sistema medicale, ossia come tale sistema svolge il suo funzionamento e in che modo tale sistema dovrà essere utilizzato.

Analizzando il documenti riportato nella tabella n.1, sono stati individuati i potenziali attori nell'adempimento dei compiti descritti dai differenti topic e subtopic.

Per semplicità sono stati definiti come:

- **Servizio Informatico** (tutte le realtà operanti a livello tecnico e gestionale sull'infrastruttura informatica ospedaliera, vedi rete, dominio etc.)
- **Servizio di Radiologia**, (tutte le realtà cliniche afferenti al sistema PACS e RIS e alla loro gestione, non solo quindi la Radiologia ma anche la Fisica Sanitaria e gli eventuali altri reparti che producono o utilizzano immagini attraverso il PACS)
- **Fornitore SW** (la o le società fornitrici dei sistemi informatici, sia HW che SW, e quelle che si occupano della loro manutenzione. Qui vengono contemplate sia le attività di installazione che quelle di gestione)

In molti casi si è ritenuto opportuno attribuire responsabilità condivise tra i differenti attori poiché alcune funzionalità del sistema (Fornitore) devono essere calate nel contesto clinico di utilizzo (Servizio di Radiologia) nonché nell'infrastruttura informatica aziendale con le proprie policy (servizio Informatico)

Tab.1

DOCUMENTAZIONE DEL PRODUTTORE			Servizio Informatico	Servizio di Radiologia	Fornitore SW
TOPIC	sub TOPIC	Contenuto			
Informazioni generali	Documentazione	Usò previsto del dispositivo in ambiente collegato in rete			X
		Istruzioni per l'installazione e l'assistenza che descrivono chi (operatore, tecnico dell'assistenza) è responsabile di quali attività e con quale frequenza devono essere eseguite.			X
		Elenco delle istruzioni per l'uso che specificano quali attività l'operatore deve svolgere, nonché come e con quale frequenza devono essere eseguite.			X
Valutazione del rischio	Rischi SI	Descrizione delle minacce alla sicurezza SI e delle conseguenze per i pazienti, gli utenti e i terzi.	X		X
	Regolamento generale per la protezione dei dati	Analisi dei rischi e valutazione dell'impatto sulla protezione dei dati (art. 25, 32, 35 GDPR)	X	X	X
	Sicurezza	Descrizione degli effetti delle funzioni rilevanti per la sicurezza (in termini di pericoli)	X		X
Autenticazione e autorizzazione	Ruoli	Elenco di tutti i ruoli che sono direttamente o indirettamente coinvolti nell'uso o nella gestione del dispositivo medico	X	X	
	Profili	Descrizione del profilo dei ruoli	X	X	X
	IAM	Descrizione dell'identità e del sistema di gestione degli accessi	X	X	X
Rete	Interfacce di rete	Elenco di tutte le interfacce dati (ad es. cablate, WLAN, USB, ecc.)	X		X
	Architettura di rete	Schema di rete che indica le connessioni ad altri componenti del sistema o risorse esterne	X	X	X
	Sicurezza di rete	Test di sicurezza. Descrizione dei test di vulnerabilità e di penetrazione del sistema eseguiti.	X		X
Dati	Mappatura dei dati	Elenco di tutti i dati gestiti dal sistema relativi allo schema dell'architettura del software		X	X
	Mappatura del flusso dei dati	Schema del flusso dei dati e dei protocolli che indica le connessioni ad altri componenti del sistema o a risorse esterne	X	X	X

DOCUMENTAZIONE DEL PRODUTTORE			Servizio Informatico	Servizio di Radiologia	Fornitore SW
TOPIC	sub TOPIC	Contenuto			
Attività di lavorazione	Registri delle attività di elaborazione	Art. 30 PILR. Attività di processo relative allo schema dell'architettura del software			X
Sistema	Interfacce di sistema	Elenco di tutti i sistemi vicini (ad es. dispositivi medici, sistemi SI) che possono essere collegati al prodotto.	X	X	X
	Architettura del sistema	Schema dell'architettura del sistema relativo allo schema dell'architettura di rete	X		X
	Sicurezza del sistema	Patch e gestione delle vulnerabilità. Piano di applicazione e rimozione delle patch. Questo piano include lo sviluppo, la distribuzione, l'installazione e la revisione delle patch.	X		
		Descrizione del software anti-malware approvato per il prodotto, dove (ad es. link) può essere ottenuto e chi è responsabile del suo aggiornamento.	X		X
		Istruzioni su come trattare gli elementi di autenticazione smarriti o rubati (ad es. carte, certificati, chiavi crittografiche) e le password dimenticate.	X		X
		Test di sicurezza. Descrizione della vulnerabilità del sistema eseguita		X	
Software	Mappatura dei software	Elenco (e descrizione) di tutti i software che implementano il sistema			X
	Architettura dei software	Schema dell'architettura del software relativo allo schema dell'architettura del sistema			X
	Sicurezza dei software	Test di sicurezza del software. Descrizione della sicurezza del software eseguito (ad es. test di penetrazione).	X	X	X
Monitoraggio	MonitoraggioSI	Descrizione del monitoraggio del SI e delle modalità di implementazione.	X	X	
	Avvisi di allarme	Descrizione del limite di soglia di allarme (avviso, errori) e dei relativi KPI sono stati impostati. Descrizione di come il dispositivo medico informa gli utenti in caso di violazione dei dati e/o di compromissione della sicurezza informatica			X
Gestione degli incidenti	Piano di risposta agli incidenti	Descrizione del piano di risposta all'incidente	X	X	X
	Procedura in caso di Data Breach	Violazione dei dati personali. Art. 33 PILR	X		X
	Contatti	I dati di contatto del produttore da utilizzare, ad esempio, in caso di problemi di sicurezza informatica			X

Informazioni generali

Documentazione

Il primo macro argomento all'interno del documento riguarda le **informazioni generali** fornite dalla *documentazione*, ossia:

- l'uso previsto del dispositivo all'interno di una rete,
- le istruzioni per l'installazione del sistema,
- quali figure professionali sono responsabile di determinate attività, e con quale frequenza tali attività devono essere eseguite.

Tali indicazioni sono definite dal fornitore del software.

Valutazione del rischio

All'interno della **valutazione del rischio** si analizzano i *rischi per il SI*, il *regolamento generale per la protezione dei dati*, e la *sicurezza*, di cui se ne occupa il servizio informatico (SI) . Tuttavia l'analisi del rischio deve essere un'attività condivisa con tutti gli attori afferenti al sistema.

Rischi SI

I rischi per il SI sono minacce alla sicurezza del sistema, ed a pazienti, utenti e terze persone.

Regolamento generale per la protezione dei dati

Si effettua l'analisi dei rischi e la valutazione dell' impatto sulla protezione dei dati, secondo gli art. 25, 32, 35 GDPR.

Sicurezza

Dedicata alla descrizione degli effetti delle funzioni rilevanti per la sicurezza, in termini di pericoli.

Autenticazione e autorizzazione

Al servizio informatico è demandata anche **l'autenticazione e l'autorizzazione dei profili** coinvolti nella gestione dei dispositivi. Ovviamente queste procedure devono coinvolgere ed essere concordate secondo logiche cliniche e funzionali con il fornitore SW e con il servizio di radiologia (SR).

Ruoli

I ruoli vengono individuati dal SW e successivamente calati nel contesto clinico, questi si devono integrare con le policy aziendali di autenticazione e gestione degli utenti di dominio, ad esempio.

Profili

Si fornisce una descrizione dettagliata del profilo dei ruoli, descrivendone dunque le competenze.

IAM (sistema di gestione degli accessi)

Descrizione delle modalità con cui deve essere utilizzato lo IAM.

Rete

E' demandata al Servizio Informatico la competenza sulle **reti informatiche e la loro gestione fino ai device del fornitore.**

Interfacce di rete

Il SI si incarica di fornire l'elenco di tutte le interfacce di rete, come ad esempio le reti cablate, WLAN ecc.

Architettura di rete

Il SI fornisce uno schema dell'architettura di rete, all'interno del quale sono mostrate tutte le connessioni che il sistema avrà con altri componenti del sistema o con risorse esterne.

Sicurezza di rete

Il SI si occupa di verificare la sicurezza della rete, eseguendo dei test, dai quali risultati scaturiranno la vulnerabilità e il rischio penetrazione del sistema. Questo aspetto, come molti altri deve essere condiviso con il fornitore al fine di evitare conflitti o falle.

Gestione dei dati

Mappatura dei dati

Il servizio di radiologia ed il fornitore si incaricano di stilare un elenco di tutti i dati gestiti all'interno del sistema, relativi allo schema dell'architettura del software e la loro modalità di immissione.

Mappatura del flusso dei dati

Il servizio informatico e il fornitore si occupano di fornire uno schema del flusso dei dati e dei protocolli, all'interno del quale sono mostrate le connessioni ad altri componenti del sistema o a risorse esterne.

Attività di lavorazione

Registri delle attività di elaborazione

Il SR produce dei registri (anche virtuali, es *log*) delle attività di elaborazione, in cui vengono elencate le attività di processo relative allo schema dell'architettura del software. Questa attività si definisce in base alle risorse e alla funzionalità del SW.

Sistema

Interfacce di sistema

Sono descritti quali sistemi (limitrofi al sistema che verrà installato), possono essere collegati a quest'ultimo, tale decisione è presa in concomitanza dal SR in cui verrà installato il nuovo sistema, e dal fornitore SW.

Architettura del sistema

Il SI e fornitore si occupano di produrre uno schema dell'architettura del sistema relativo allo schema dell'architettura di rete.

Sicurezza del sistema

Il servizio informatico si incarica di:

- descrivere le caratteristiche che il software anti-malware deve avere, dove tale software può essere ottenuto, e quale figura professionale deve occuparsi del suo aggiornamento (sia interno all'AO che esterno, in relazione al sistema su cui va installato).
- Descrivere il procedimento da svolgere in caso di elementi di autenticazione smarriti, quali password dimenticate, chiavi crittografiche ecc.

Il SI e il fornitore si accordano sulle modalità di distribuzione, installazione ed applicazione delle patch, e di eseguire i test di sicurezza, conservando i risultati utili a descrivere le vulnerabilità del sistema.

Software

Il fornitore si occupa di tutti gli aspetti relativi appunto al **software**, ossia la *mappatura dei software*, *l'architettura dei software*, e la *sicurezza* di questo.

Mappatura dei software

Per mappatura dei software si intende l'elenco e la descrizione di tutti i software che implementano il sistema.

Architettura dei software

Per descrivere l'architettura dei software è necessaria la stesura di uno schema relativo all'architettura del sistema.

Sicurezza dei software

Per garantire la sicurezza dei SW è necessaria l'esecuzione dei test di sicurezza e la descrizione della sicurezza del software. Questi aspetti possono essere condivisi sia con il SR che con il SI.

Monitoraggio

Del **monitoraggio** del sistema se ne occupano il servizio informatico ed il fornitore.

Monitoraggio SI

Il SI è incaricato del monitoraggio e della descrizione delle modalità di implementazione.

Avvisi di allarme

Il fornitore si incarica della descrizione di come il dispositivo medico informa gli utenti in caso di violazione dei dati e compromissione delle sicurezza informatica.

Gestione degli incidenti

Piano di risposta agli incidenti

Tutti gli attori coinvolti devono concordare un piano di risposta rapida ad un eventuale incidente.

Procedura in caso di Data Breach

Il SI e il fornitore sono incaricati della descrizione della procedura da eseguire in caso di violazione dei dati personali.

Contatti

Il fornitore fornisce i dati del contatto del produttore da utilizzare in caso di problemi di sicurezza informatica.

Capitolo 4 : Norme di buon utilizzo RIS-PACS del Tecnico

Sanitario di Radiologia Medica

Secondo l'art. 14 del codice deontologico, in un ambiente lavorativo è fondamentale prevenire e gestire eventuali errori; tali errori possono essere sfruttati per migliorare l'organizzazione attraverso procedure professionali più idonee.

L'errore è contemplato come evento possibile, e possibili modi di errore, sono sempre oggetto di analisi e verifica.

La metodologia che si occupa dell'analisi sistematica degli errori, al fine di ridurli al minimo, è l'audit.

L'audit prevede il confronto sistematico dell'assistenza prestata, al fine di individuare differenze rispetto gli standard.

Fine ultimo dell'audit dunque è l'attuazione di cambiamenti funzionali alla riduzione dell'errore, ed il monitoraggio di tali misure correttive introdotte.

Precisamente, i compiti dell'audit clinico possono riassumersi in:

- identificare i rischi correlati alla attività clinica e all'organizzazione;
- identificare errori e quasi eventi;
- identificare le cause, i fattori contribuenti e concomitanti di eventi avversi;
- identificare gli ambiti di miglioramento.

L'errore in ambito medico, può essere classificato come:

- errore attivo, il quale avviene in un lasso di tempo prossimo all'evento avverso, ed è riconducibile ad un'azione eseguita in modo sbagliato da un operatore, oppure ad un incidente, quale potrebbe essere il malfunzionamento di uno strumento;
- errore latente, il quale nasce da insufficienze organizzative e gestionali del sistema, la cui conseguenza è il verificarsi di un errore attivo.

Definiamo un evento avverso, come un evento inatteso, correlato al processo assistenziale, che comporta un danno al paziente, non intenzionale ed indesiderabile.

Possiamo classificare gli eventi avversi come prevenibili, e non prevenibili; gli eventi avversi che scaturiscono da un errore, sono tali da essere classificati come eventi avversi prevenibili.

Al fine di evitare che tali errori si ripetano, vengono analizzate le insufficienze nel sistema che contribuiscono allo scatenarsi di un evento avverso, inoltre si progettano contromisure tali da impedire il suddetto evento.

Vi sono principalmente due approcci all' analisi del rischio:

- approccio proattivo, che prevede la revisione dei processi e delle procedure esistenti, con l'obiettivo di individuare eventuali criticità; tale approccio è valido anche nella progettazione di nuove procedure, per realizzare barriere protettive che impediscano l'errore umano;
- approccio reattivo, che prevede l'analisi di un evento avverso e la conseguente ricostruzione a ritroso dei fatti, con il fine di individuare le cause dell'evento avverso.

4.1: Case Report : analisi e correzione

4.1.1 Caso di omonimia al Sant'Orsola di Bologna

Il 5 luglio 2007, la Sig.ra L. Daniela, di 54 anni, si presenta al Pronto Soccorso dell'Azienda Ospedaliero- Universitaria/Policlinico S. Orsola - Malpighi di Bologna, lamentando una lombalgia sinistra.

La Sig.ra Daniela viene sottoposta ad un'ecografia, il cui responso è una lieve dilatazione dell'uretere di sinistra e la presenza di angiomiolipoma renale di 13mm.

La suddetta signora ripete l'ecografia privatamente, ed ha la stessa diagnosi.

Il Medico di Medicina Generale (MMG) richiede un Uro-TC per ricercare sospetta neoplasia renale, tale Uro-TC viene prenotata tramite CUP, ed eseguita il 13 agosto 2007.

Al termine dell'esame TC, l'intero studio viene inviato al server del PACS.

Il 14 agosto, il giorno seguente, la Sig.ra Teresa, omonima per cognome rispetto la Sig.ra Daniela, si sottopone ad Uro-TC.

Le immagini mostrano una neoplasia del segmento pre-vescicale dell'uretere sinistro con conseguente idro-ureteronefrosi di III-IV grado.

Sia nel giorno 13 agosto, che nel 14 agosto, è di turno lo stesso TSRM, mentre il Medico Radiologo è diverso da un giorno all'altro.

Le immagini dello studio TC della signora Teresa vengono inviate al doppio server del PACS, ma vengono attribuite per sbaglio, alla signora Daniela, la quale aveva eseguito l'Uro-Tc il giorno prima, ed era ancora presente nella worklist della consolle, nella riga precedente di quella della Sig.ra Teresa.

Il TSRM si accorge subito dell'errore, e sulla consolle della TC i dati anagrafici e l'ID paziente della Sig.ra Daniela vengono corretti con quelli della Sig.ra Teresa, e l'intero studio viene inviato al PACS.

Successivamente, il TSRM interviene sui due server (PACS e PACS web), con l'obiettivo di eliminare le immagini errate, ossia quelle della signora Teresa, inviate ed attribuite erroneamente alla signora Daniela.

Dalla postazione PC dietro la consolle, il TSRM accede al server del PACS, e verifica che compaiono a nome della signora L. Daniela due esami, eseguiti in giorni diversi, 13 e 14 agosto.

A questo punto il TSRM esegue la cancellazione, sbagliando però nel selezionare l'esame sul server PACS, mentre esegue correttamente la stessa azione nel server WEB.

Perciò, sul server del PACS che è consultato dal reparto di radiologia, e tramite il quale si inviano le immagini ai masterizzatori dei CD, vengono cancellate le 1585 immagini del vero esame della signora Daniela, acquisite il 13 agosto mentre rimangono sul server PACS solo le 1641 della signora Teresa acquisite il 14 agosto, ma attribuite erroneamente a L. Daniela.

Sul server WEB, tramite il quale le immagini vengono diffuse a tutto l'ospedale, viene eseguita correttamente la cancellazione della sequenza sbagliata, e restano disponibili le vere immagini della signora Daniela.

Il TSRM, che aveva svolto altre volte il compito, non ha informato il medico radiologo del suo intervento di manutenzione sui server PACS, in quanto il protocollo operativo non obbligava il TSRM ad allertare il radiologo.

Un secondo radiologo, diverso da quello in turno nel giorno 13 agosto, referta lo studio TC della Sig.ra Teresa il 17/08 e le diagnostica un quadro di idroureteronefrosi sinistra di III grado per stenosi neoplastica dell'uretere distale aggettante in vescica, consigliando un completamento cistoureteroscopico.

Invece, il medico radiologo in turno il giorno 13 agosto, referta lo studio TC della Sig.ra Daniela (sulle immagini sbagliate della signora Teresa, ma con i dati anagrafici corretti della signora Daniela, con la sola discrepanza di data sulle immagini).

Lo studio viene refertato il 17/08, dopo 4 giorni dall'esecuzione dell'esame, ed ovviamente nel referto si descrive lo stesso quadro diagnostico della Sig.ra Teresa, ossia idroureteronefrosi sinistra di III grado per stenosi neoplastica dell'uretere distale aggettante in vescica, con conseguente richiesta di completamento cistoureteroscopico.

Inoltre i due radiologi si erano confrontati sullo studio di L. Daniela, poiché il radiologo che aveva refertato recentemente L. Teresa era ritenuto più esperto in casi di urologia; quest'ultimo però non si è accorto che il caso di L. Daniela presentasse le stesse caratteristiche (ed immagini) di quello di L. Teresa, da lui refertato.

La signora Daniela ritira inoltre, insieme al referto, il CD, il quale conteneva però le immagini TC errate.

Viene, dunque eseguita una cisto-ureteroscopia alla Sig.ra L. Daniela, dagli stessi urologi che in seguito si occuperanno dell'operazione.

Il quadro cistoscopico negativo, porta l'urologo a non ritenere opportuno l'esecuzione dell'ureteroscopia.

L'urologo, perplesso a causa della discordanza tra i reperti TC (positivi) ed i reperti cistoscopici ed ecografici (negativi), chiede ad un collaboratore di recarsi in radiologia, al fine di verificare le immagini contenute nel CD e di richiedere una consulenza radiologica.

La consulenza viene fornita da un terzo radiologo, estraneo al caso sino a quel momento, che verifica sul PACS la patologia e la discordanza tra i referti TC e quelli delle altre metodiche diagnostiche.

Senza ulteriori accertamenti diagnostici, l'urologo decide comunque di effettuare una nefroureterectomia.

L'intervento viene eseguito per via laparoscopica, dopo aver clampato e sezionato i vasi renali, l'urologo si rende conto di essere di fronte ad un quadro renale non patologico, con assente dilatazione dell'uretere (che, invece nelle immagini TC presenti nel CD appariva dilatato).

Le immagini TC presenti nel CD sono state l'unica metodica valutata in fase preoperatoria.

A questo punto l'urologo decide di ricercare sul WEB il caso clinico, e si trova di fronte alle "immagini giuste", le quali mostravano una condizione (negativa) completamente diversa da quella presente sul CD.

Essendo ormai l'intervento in fase avanzata, viene comunque completata la nefrectomia del rene sano.

La Sig.ra L. Daniela viene informata dell'accaduto il giorno successivo, dalla Direzione dell'U.O.

La mattina seguente, la paziente decede in seguito a sopraggiunta embolia polmonare, dopo aver mostrato episodi dispnoici premonitori, durante la notte antecedente.

Alla signora Daniela, non era stato somministrato alcun anticoagulante, ma l'urologo, falsificando la cartella, scrive della somministrazione di Clexane.

I principali punti critici della vicenda sono :

Preliminari

1. Prenotazione CUP di esame inappropriato (carente giustificazione preliminare)
2. Elevati carichi di lavoro Sezione TC (18-20 es. nel Turno di 6 ore e 20')
3. Organico medico ridotto (periodo 12-19 agosto)
4. Scarsa diffusione della "cultura del rischio"

Nel Fatto

1. Omonimie nel cognome delle pazienti
2. Persistenza nella worklist dei pazienti inseriti ed effettuati nei 3 giorni precedenti
3. Cancellazione delle immagini del vero esame e cambio d'attribuzione alla paziente omonima nel PACS server (ma persistenza delle immagini con corretta attribuzione nel Web-server)
4. Mancata informazione del medico radiologo di tale cancellazione
5. Consulto tra i due colleghi refertanti i due casi omonimi scambiati, senza riconoscimento che si trattava del medesimo caso
6. Referto radiologico stilato dopo 4 giorni dall'esame sulle immagini scambiate
7. Successivo consulto estemporaneo tra medico specialista ed un terzo radiologo
8. Mancata consultazione del caso sul web-server, preliminarmente all'intervento, da parte dell'urologo
9. Modalità d' intervento chirurgico (via laparoscopica vs chirurgia tradizionale)
10. Mancata somministrazione terapia anticoagulante in paziente a rischio tromboembolico (obesità)

Dall'analisi dell'evento avverso, sono state attuate contromisure il cui intento è evitare che si ripetano tali eventi avversi.

- E' stato inserito un meccanismo all'interno del RIS che prevede un messaggio di allerta in caso di omonimie;
- E' stato inserito un tasto di invio alla worklist della TC, dopo aver identificato il paziente su RIS;
- E' stata semplificata l'interfaccia grafica della worklist della TC, la quale mostra solo il nominativo del paziente in studio;
- La ditta fornitrice dei server PACS e WEB ha provveduto ad abilitare l'allineamento automatico tra i due server, al fine di evitare discrepanze come nel caso del S. Orsola;

- Sono stati individuati 7 TSRM, definiti con il ruolo di esperto informatico di radiologia, che dopo specifica formazione, si dedicano esclusivamente allo svolgimento di compiti, come cancellazione esami dal PACS, allineamenti degli ID, e correzioni di errate assegnazioni;
- Sono stati ridotti il numero di esami TC per turno lavorativo, passano ad un massimo di 13 pazienti programmati, più eventuali 2-3 urgenze;
- E' stata disposta la pianificazione per l'uso delle Workstation di refertazione, con diritto di prelazione nel pomeriggio per chi ha appena finito il turno TC della mattina;
- E' stata introdotto un lasso di tempo dedicato al consulto su vari casi clinici, nell'arco della turnazione dei medici.

4.1.2 Caso di errata fusione paziente presso l'Azienda Ospedaliero Universitaria Ospedali Riuniti di Ancona

Il giorno 01/08/2018 la Sig.ra T.B. nata nell'anno 1963, si presenta presso l'Azienda Ospedaliero Universitaria Ospedali Riuniti di Ancona) per effettuare una mammografia bilaterale.

In fase di refertazione, subito dopo l'indagine mammografica, il medico Radiologo si accorge che alcune immagini degli esami mammografici svolti in precedenza dalla Sig.ra nell'arco temporale 2011-2017 risultano associate ad un'altra signora, omonima per nome e per cognome, ma nata in luogo differente ed in un anno differente (nel 1952). (Fig.20)

Patient Name	Patient ID	Patient Birthd...	Procedure	Mdl	Img	Study Time	Online	Status
Cognome_Nome	RM 04	1963	MAMMOGRAFIA BILA...	DX	4	2005.12.06 15:11:03	N	Completed
Cognome_Nome	RM 04	1963	MAMMOGRAFIA BILA...	DX	4	2007.03.01 17:03:44	N	Completed
Cognome_Nome	RM 04	1963	ECOGRAFIA MAMMAR...	US	0	2007.03.01 16:40:00	N	Completed
Cognome_Nome	RM 04	1963	MAMMOGRAFIA BILA...	DX	4	2008.06.09 15:44:52	N	Completed
Cognome_Nome	RM 04	1963	ECOGRAFIA MAMMAR...	US	0	2008.06.09 15:36:51	N	Completed
Cognome_Nome	RM 04	1963	MAMMOGRAFIA BILA...	DX	4	2009.08.05 11:41:34	N	Completed
Cognome_Nome	RM 04	1963	ECOGRAFIA MAMMAR...	US	0	2009.08.05 11:20:00	N	Completed
Cognome_Nome	RM 04	1963	MAMMOGRAFIA BILA...	DX	4	2010.08.06 08:42:18	Y	Completed
Cognome_Nome	RM 04	1963	ECOGRAFIA MAMMAR...	US	0	2010.08.06 08:10:00	N	Completed
Cognome_Nome	RM 04	1963	RX mammografia bila...	MG	4	2010.08.01 11:15:15	Y	Completed
Cognome_Nome	RM 04	1963	Ecografia mammaria ...	US	0	2010.08.01 10:35:00	N	Completed
Cognome_Nome	RM 59	1952	MAMMOGRAFIA BILA...	DX	4	2011.11.04 11:30:41	Y	Completed
Cognome_Nome	RM 59	1952	ECOGRAFIA MAMMAR...	US	0	2011.11.04 11:11:39	N	Completed
Cognome_Nome	RM 59	1952	ECOGRAFIA MAMMAR...	US	0	2013.02.06 10:10:00	N	Completed
Cognome_Nome	RM 59	1952	MAMMOGRAFIA BILA...	DX	4	2013.02.06 11:06:20	Y	Completed
Cognome_Nome	RM 59	1952	RM addome inferiore ...	MR	150	2013.04.10 11:21:57	N	Completed
Cognome_Nome	RM 59	1952	MAMMOGRAFIA BILA...	DX	4	2014.05.29 10:47:41	Y	Completed
Cognome_Nome	RM 59	1952	ECOGRAFIA MAMMAR...	US	0	2014.05.29 09:50:00	N	Completed
Cognome_Nome	RM 59	1952	MAMMOGRAFIA BILA...	DX	4	2015.11.23 09:20:12	Y	Completed
Cognome_Nome	RM 59	1952	ECOGRAFIA MAMMAR...	US	0	2015.11.23 08:36:00	Y	Completed
Cognome_Nome	RM 59	1952	MAMMOGRAFIA BILA...	DX	4	2017.03.22 18:03:14	Y	Completed
Cognome_Nome	RM 59	1952	ECOGRAFIA MAMMAR...	US	0	2017.03.22 17:15:00	N	Completed

Fig.20 Associazione errata di alcuni esami mammografici

Il problema di errata fusione è presente sul sistema RIS ospedaliero.

Per controprova si decide di verificare se la signora T.B. nata nel 1952, sia stata sottoposta a mammografia bilaterale presso gli Ospedale Riuniti negli anni precedenti all'ultimo esame.

Ad un'analisi effettuata sul sistema RIS in uso presso l'azienda prima dell'adozione di quello attuale risulta che la Sig.ra T.B. nata nel 1952, non è stata mai sottoposta ad esami radiografici presso la struttura. (Fig. 21)

ID paz. HIS paziente	Cogn. paz	Nome paziente	Dal.nasc.	Esame	Nome esame	Stato	Staz.lav	Inizio esame prog.	Descr. tipo ricor.	Abbrev.richied.	Sez.ist.	Ist.
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	09.05.2008	18.00		Ambulatoriale	ESTERNO	DIPNOME	RADOSP
1993	P02E0102	ECO MAMMARI		val	ECOMA	09.05.2008	15.36		Ambulatoriale	ESTERNO	DIPNOME	RADQLI
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	05.12.2005	14.40		Ambulatoriale	ESTERNO	DIPNOME	RADOSP
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	05.08.2009	11.20		Ambulatoriale	ESTERNO	DIPNOME	RADOSP
1993	P02E0102	ECO MAMMARI		val	ECOMA	05.08.2009	11.20		Ambulatoriale	ESTERNO	DIPNOME	RADQLI
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	06.08.2010	08.10		Ambulatoriale	ESTERNO	DIPNOME	RADQLI
1993	P02E0102	ECO MAMMARI		val	ECOMA	06.08.2010	08.10		Ambulatoriale	ESTERNO	DIPNOME	RADQLI
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	01.03.2007	16.40		Ambulatoriale	ESTERNO	DIPNOME	RADOSP
1993	P02E0102	ECO MAMMARI		val	ECOMA	01.03.2007	16.40		Ambulatoriale	ESTERNO	DIPNOME	RADQLI
1993	P02E0102	ECO MAMMARI		val	ECOMA	23.11.2015	08.36		Ambulatoriale	ESTERNO	MAMMO	RADQLI
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	23.11.2015	08.36		Ambulatoriale	ESTERNO	MAMMO	RADQLI
1993	P02E0102	ECO MAMMARI		val	ECOMA	06.02.2013	10.10		Ambulatoriale	ESTERNO	MAMMO	RADOSP
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	06.02.2013	10.10		Ambulatoriale	ESTERNO	MAMMO	RADOSP
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	04.11.2011	11.11		Ambulatoriale	ESTERNO	DIPNOME	RADQLI
1993	P02E0102	ECO MAMMARI		val	ECOMA	04.11.2011	11.11		Ambulatoriale	ESTERNO	DIPNOME	RADQLI
1993	P04B0332	RMI addome RI		val	RMIT	10.04.2010	09.53		Ambulatoriale	ESTERNO	RIMCCL	RADOSP
1993	P02E0102	ECO MAMMARI		val	ECOMA	29.05.2014	09.50		Ambulatoriale	ESTERNO	MAMMO	RADQLI
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	29.05.2014	09.50		Ambulatoriale	ESTERNO	MAMMO	RADQLI
1993	MISSING	MISSING		rich		06.08.2013	09.10					
1993	MISSING	MISSING		rich		04.07.2013	11.00					
1993	P02E0102	ECO MAMMARI		val	ECOMA	22.03.2017	17.15		Ambulatoriale	ESTERNO	MAMMO	RADQLI
1993	P01E0102	MAMMOGRAFIA		val	MAMMO	22.03.2017	17.15		Ambulatoriale	ESTERNO	MAMMO	RADQLI
1993	MISSING	MISSING		rich		04.04.2017	15.00					
1993	MISSING	MISSING		rich		14.02.2017	15.00					
1993	P02E0102	ECO MAMMARI		rich		01.08.2018	10.36				MAMMO	RADQLI
1993	P01E0102	MAMMOGRAFIA		rich		01.08.2018	10.36				MAMMO	RADQLI
1993	MISSING	MISSING		rich		26.01.2017	15.15					

Fig.21 Verifica eseguita sul sistema RIS, precedente ad Exprivia

Il giorno stesso ed il successivo è stato chiesto alla ditta fornitrice del sistema RIS regionale di trovare e risolvere la causa dell'errore.

Da indagini sul loro sistema si è visto che l'errata fusione è stata effettuata in un altro polo ospedaliero.

Non sono stati forniti ulteriori dettagli su quando o chi abbia fatto questa operazione (Fig.22).

Nome paziente	Data Nascita	S	Luogo Nascita	Cod ARCA	Cod ASR-EMPI	Cod.Fiscale	Cod Marche Nord	URLA
T M	1963	F	SE					

Fig.22 Tramite Exprivia si risale all'origine dell'errore

In seguito si tenta di riparare all'errore cercando di associare correttamente gli esami svolti.

Dopo vari tentativi, però, due esami della Sig.ra T.B. nata nel 1963, risultano associati alla signora T.B. nata nel 1952.

Al fine di attribuire gli esami svolti alla persona giusta, vengono analizzati gli Header Dicom di tutte le immagini.

Dall'analisi emerge che le immagini precedentemente associate alla signora T.B. del 1952, sono in realtà della signora T.B. del 1963, come viene dimostrato nell'immagine sottostante. (Fig.23)

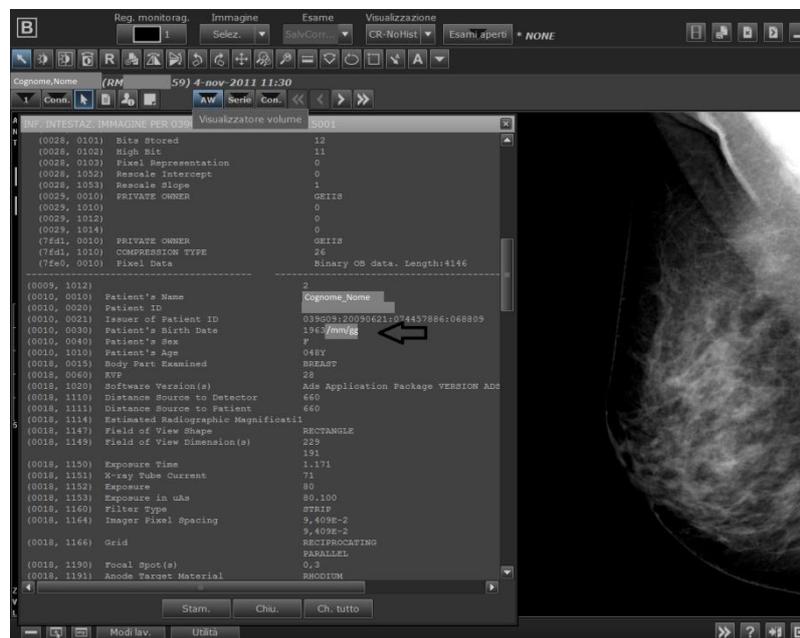


Fig.23 Analisi dell'header DICOM

In conclusione si hanno due situazioni ancora da correggere:

- su sistema RIS un esame mammografico del 2011 appartenenti realmente alla signora T.B. nata nel 1963 è ancora associato alla signora T.M. nata nel 1952 .
- su sistema PACS nulla è stato fatto in attesa di decidere se effettuare un merge manuale o automatico.

Glossario

ACR : American College of Radiology

ADT : sistema di Accettazione/Dimissione/Trasferimento

BYOD : Bring Your Own Device

CESM : Contrast Enhanced Spectral Mammography

CR : Computer Radiography

CT : Computer Tomography

CUP : Centro Unico di Prenotazione

DICOM : Digital Imaging and COmmunication in Medicine

EA : Enterprise Archive

GDPR : Regolamento Generale sulla Protezione dei Dati

HIMSS : Healthcare Information and Management Systems Society

HIS : Sistema Informativo Sanitario

HL7 : Health Level 7

HW : Hardware

IAM : Sistema di Gestione degli Accessi

IHE : Integrating the Healthcare Enterprise

ISO : Organizzazione internazionale per la normazione

IT : Dipartimento di Tecnologia dell'Informazione

MDR : Regolazione dei Dispositivi Medici

MIP : Maximum Intensity Projection

MMG : Medico di Medicina Generale

MPR : Multiplanar Reconstruction

MRI : Magnetic Resonance Imaging

NEMA : National Electrical Manufacturer Association

NISD : Direttiva sulla Sicurezza delle Reti e dell'Informazione

PACS: Picture Archiving and Communication System

RIS: Sistema Informatico Radiologico

RSNA: Radiological Society of North America

SI : Servizio Informatico

SR : Servizio di Radiologia

SW : Software

TSRM : Tecnico Sanitario di Radiologia Medica

VR : Virtual Reconstruction

WADO : Web Access to DICOM Objects

WS : Workstations

Conclusioni

Dall'analisi effettuata, una realtà articolata come quella descritta, presenta elevati livelli di rischio. Si è evidenziato che una completa ed efficace analisi dei rischi è un'attività né semplice tecnicamente né tantomeno a livello pratico organizzativo.

L'integrazione di un sistema PACS con l'infrastruttura aziendale, con le modalità diagnostiche, con le periferiche, con gli altri sistemi informatici richiedono la collaborazione di diverse professionalità non solo all'interno dell'azienda ma anche con partner esterni (come ad esempio i fornitori).

Gli aspetti critici possono essere sia strutturali che funzionali, nonché gestionali; i sistemi in quanto tali, spesso risultano sicuri, ma è la loro applicazione e il loro utilizzo in contesti clinici che determina l'insorgenza di punti deboli.

E' evidente che non sempre questi aspetti possono essere risolti o evitati, vanno comunque riconosciuti e gestiti in modo da minimizzarne gli effetti.

In questo lavoro si è inoltre evidenziato la necessità di un lavoro preliminare di raccolta documentale e definizione di elementi, strutture e competenze, in modo da favorire le fasi successive di implementazione e gestione dei punti critici.

L'attività di risk assessment deve quindi essere considerata come un'attività continuativa, che monitori l'evoluzione di ogni singolo elemento integrato, che tenga conto degli aspetti pratici funzionali e che coinvolga attivamente sia i fornitori che gli utenti che i gestori dei sistemi.

Ringraziamenti

Un sentito grazie al Prof. Alberto Mari e alla Prof. Letizia Tesei per la loro infinità disponibilità e tempestività ad ogni mia richiesta.

Grazie per avermi fornito ogni materiale utile alla stesura dell'elaborato.

Senza il supporto morale, economico ed umano dei miei genitori e di mia sorella, non sarei mai potuto arrivare fin qui.

Grazie per esserci sempre stati, soprattutto nei momenti difficili.

Ringrazio i miei colleghi, i miei amici più stretti e tutti coloro che mi sono stati accanto in questo periodo intenso e per gioire, insieme a me, dei traguardi raggiunti.

Grazie a tutti, senza di voi non ce l'avrei mai fatta!

Sitografia

- <https://www.aiic.it/aiic/corsi/corsi-xv-convegno/>
- <https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services>
- https://www.corriere.it/cronache/07_settembre_28/rene_tac_bologna_ors_ola.shtml

Bibliografia

- Documentazione interna all'ospedale
- Documentazione fornita dalla ditta
- Materiale didattico fornito dal professor A.Badaloni relativo al modulo
SISTEMI INFORMATICI IN AMBITO RADIOLOGICO