Università Telematica Pegaso

Master in
Amministratore di sistema in ambito sanitario
(MA150)

Sicurezza, Privacy e Strumenti per il corretto utilizzo di una Rete Informatica in ambito ospedaliero.

RELATORE:

Ing. Emanuele DE LUCIA

CANDIDATO:

Antonio DI LASCIO

Matr. 1500048

Anno Accademico
2012-2013

"*Siate soprattutto uomini.*
Fino in fondo
Anzi fino in cima
Perché essere uomini fino in cima
Significa essere santi.
Non fermatevi, perciò, a mezza costa:
la santità non sopporta misure discrete"

(Don Tonino Bello, Vescovo di Molfetta, 1990)

A quanti hanno contribuito alla mia formazione umana e professionale,

alla mia Famiglia,

e a Dadda mia futura sposa.

25 ottobre 2013

INTRODUZIONE

I sistemi informativi hanno la funzione di coordinare la raccolta, la gestione e lo scambio di informazioni all'interno di una struttura sanitaria mediante l'utilizzo di un Sistema Informatico che è la componente automatizzata del Sistema Informativo.

Negli ultimi interventi, affrontando le tematiche della Semplificazione e della Sanità Digitale, il Legislatore[1], ha contribuito all'ulteriore sviluppo della Gestione Elettronica in Ambito Sanitario, affrettando quel processo di migrazione dei servizi sanitari verso una gestione, prevalentemente o interamente, informatizza. Infatti, alcuni Processi e Pratiche Cliniche di "produzione di salute", tradizionalmente caratterizzati da supporti cartacei (come ad es. la cartella clinica elettronica o sistemi di prenotazione elettronica per l'accesso alle strutture da parte dell'utenza), sono passati, o stanno passando, alla completa gestione elettronica con innumerevoli vantaggi per il flusso informativo in ambito ospedaliero, come ad esempio la possibilità della disponibilità di tutte le informazioni sanitarie in tempo reale, oppure la completezza informativa nelle pratiche dell'Utenza che afferisce, la standardizzazione dei formati, l'abbattimento dei costi e risorse per le archiviazioni, dovute per legge e dei relativi volumi. Da questi vantaggi ne consegue una maggiore efficienza per l'organizzazione accompagnata da "nuove prestazioni", finora difficilmente immaginabili, con una gestione tradizionale delle informazioni nelle nostre strutture ospedaliere, naturalmente nel rispetto della disciplina giurisprudenziale applicabile, ai medesimi servizi resi in via tradizionale, come la sicurezza e il la tutela della privacy.

[1] Disposizioni Urgenti in Materia di semplificazione e di sviluppo: D.L. n. 5 del 9/2/12; Semplificazione in Materia di Sanità Digitale: L. 4/4/2012 nr. 35

Ad oggi, la maggior parte delle informazioni (dalle Immagini Radiologiche ai Referti), sono custodite e veicolate nella struttura sanitaria attraverso modalità e supporti informatici sempre più sofisticati e performanti, la cui inevitabile condivisione, è permessa da infrastrutture rappresentate dalle Reti Informatiche (o Informatica Distribuita) di cui gli ospedali (o le strutture sanitaria) ne sono ampiamente dotati.

Per garantire costantemente la sicurezza dell'informazione, in un contesto dove i rischi informatici (causati da violazione dei sistemi di sicurezza) o errori sono in continuo aumento, è opportuno adottare politiche organizzative e accorgimenti informatici, le cui soluzioni, oggi percorribile, sono molteplici. Per garantire il corretto utilizzo di una rete informatica e il rispetto di tutti requisiti di sicurezza e privacy previsti, oltre agli accorgimenti informatici Hardware e Software, sono indispensabili "***politiche organizzative***". Strumenti utili a garantire contemporaneamente il corretto funzionamento e la sicurezza della rete informatica sono:

- L'adozione di un adeguato ***Sistema di Gestione della Sicurezza delle Informazioni (SGSI)*** finalizzato ad una corretta gestione dei dati sensibili della struttura. Attraverso lo standard ISO 27001:2005, che rappresenta un SGSI, infatti è possibile la protezione dei dati e delle informazioni da minacce di ogni tipo ed errori, al fine di assicurare l'integrità, la riservatezza e la disponibilità delle informazioni;
- siccome la sicurezza informatica è in realtà sicurezza dell'informazione, altro elemento sul quale dover dedicare attenzione è il fattore umano: che rappresenta la vera strategia che può e deve essere gestita, nel senso nobile del termine, grazie ad opportuni programmi di formazione e addestramento, prendendo in considerazione le peculiarità offerte dalla ***Certificazione ECDL Health***.

1. L'INFORMATICA IN SANITÀ

§ 1.1 Sistemi Informativi e Sistemi Informatici

In ambito ospedaliero, ciascun professionista, per fare bene il proprio lavoro, ha bisogno di acquisire informazioni utili per interpretare le problematiche e analizzare le imprevedibili dinamiche dell'ambiente sanitario al fine di prendere le decisioni più appropriate ed averle a disposizione nel momento opportuno.

In ogni azienda sanitaria, per questo, esiste un sistema informativo, che è *"l'insieme delle persone, delle tecnologie e dei meccanismi operativi il cui compito è quello di raccogliere, archiviare ed elaborare le informazioni che servono all'attività dell'azienda e alla sua gestione. In altri termini scopo del sistema informativo è quello di fornire a ogni componente dell'organizzazione tutte le informazioni di cui ha bisogno per il migliore svolgimento del suo mandato*"[2].

Il sistema informativo aziendale nella maggior parte dei casi si avvale di elaboratori elettronici realizzando il così detto ***sistema informatico aziendale***, porzione del sistema informativo, inteso come "*l'insieme delle risorse umane e tecniche e di procedure che consente il trattamento automatico dei dati*"[3].

Grazie all'evoluzione tecnologica in corso in questi ultimi anni le aziende sanitarie stanno maturando esperienze significative, nel campo informatico ed informativo, potendo disporre di strumenti sempre più efficienti ed efficaci, a supporto delle loro attività ed esigenze di tipo amministrativo, organizzativo e clinico.

2 C. Calamandrei, C. Orlandi "La Dirigenza infermieristica. Manuale per la formazione dell'infermiere con funzioni manageriali", ed. Mc-Graw-Hill, Milano 2009 III edizione, cap. 13 pag. 236

3 G. Donna, S. Nieddu, M. Bianco "Management Sanitario. Modelli e strumenti per gli operatori delle aziende sanitarie", ed. Centro Scientifico Editore, Torino 2003, Cap. 13 p. 293

Elemento decisivo di questa evoluzione tecnologica è stato lo sviluppo dei Personal Computer, che hanno reso disponibili computers sempre più piccoli e meno costosi, dotati di grandi prestazioni e tra di loro collegabili in reti locali, autonome o meno dall'intero sistema ospedaliero. Le reti locali costituiscono un'applicazione dell'informatica distribuita, che deve essere intesa come "*condivisione di archivi e programmi attraverso la rete, mantenendo però l'autonomia e la capacità di calcolo di ogni personal computer collegato*"[4].

§ 1.2 L'Information and Communication Technology

La presenza di enormi quantità di informazioni e documenti hanno reso sempre più necessaria l'adozione di applicazioni e strumenti per la gestione dei processi e l'accesso alle informazioni sanitarie da parte dei diversi operatori nei processi di "fornitura di salute". Questo ha reso necessario dotarsi di soluzioni per lo scambio dei dati e l'interoperabilità dei servizi applicativi, anche nel quadro di sistemi sanitari regionali e nazionale (es. Fascicolo Sanitario Elettronico), con strumenti in grado di abilitare e sostenere processi di rivelazione, analisi e valutazione dei parametri, legati all'attività e ai risultati perseguiti dalla organizzazione sanitaria.

Con l'acronimo Information and Communication Technology (ICT) si intende "*l'insieme delle tecnologie che consentono il trattamento (archiviazione, elaborazione e trasformazione) e lo scambio delle informazioni, siano esse testuali, visive o sonore, in formato digitale*"[5].

"L'introduzione degli strumenti di ICT offre in ambito sanitario, in particolare al personale afferente l'area clinica (medici, infermieri, tecnici) la possibilità di

[4] F. Mazzucato "Anatomia Radiologica. Tecnica e metodologia in radiodiagnostica", ed. Piccin, Padova 2009, III edizione Cap. 2 (Battaglia, Maroldi) p. 100

[5] da Wikipedia L'enciclopedia libera. Ricerca: "Tecnologie dell'informazione e della comunicazione" ultimo accesso 12/8/2013 http://it.wikipedia.org/wiki/Information_and_Communication_Technology

migliorare le proprie prestazioni e quindi l'erogazione del servizio all'utente attraverso:

- *una riduzione dei tempi di svolgimento di attività di immissione dati, grazie alla condivisione delle stesse informazioni tra tutti i reparti, che consente l'imputazione di un dato a un paziente una sola volta;*
- *una riduzione dei tempi di erogazione accelerati dal passaggio informatico delle informazioni, più veloce rispetto a quello tradizionale;*
- *un maggiore controllo sul processo, garantito dalla più intensa integrazione tra reparti e servizi che possono quindi effettuare controlli incrociati;*
- *tracciabilità delle attività e responsabilità degli operatori lungo tutte le fasi del processo;*
- *una maggiore disponibilità di informazioni che consentono di avere più elementi per poter approdare a diagnosi più complete e corrette"*[6].

Il sistema PACS, *Picture archiving and communication system* (Sistema di archiviazione e trasmissione di immagini) è un tipico esempio di ICT tra i più utilizzati in ambito sanitario che consente l'archiviazione digitale delle immagini radiologiche e la loro trasmissione e visualizzazione a distanza su workstation dedicate, collegate attraverso l'utilizzo di una rete informatica. L'architettura PACS è basata su una rete in grado di connettere le apparecchiature per l'acquisizione di immagini, le stazioni di visualizzazione/elaborazione con un archivio digitale.

Altri esempi di supporti ICT maggiormente diffusi in sanità sono:

6 AA. VV. Ricerca: "L'impatto dell'informatizzazione sulle Aziende Sanitarie Lombarde e le relative implicazioni sulla formazione e addestramento degli operatori", Fondazione ISTUD per la cultura d'impresa e di gestione, Milano Dicembre 2003. http://www.istud.it/up_media/ricerche/equal_san.pdf ultimo accesso 12/08/2013

- clinical decision supporty system (CDSS): fornisce agli operatori sanitari (medici ed infermieri) in tempo reale informazioni su linee guida e protocoli clinico-assistenziali, prontuario farmaceutico;
- Radio Frequency Identification (RFID): tracciamento del paziente in tutto l'ospedale in tutti le risorse di afferenza;
- Automated Dispensing Machines (ADMs): distruzione automatizzata di dosi di farmaci;
- Elettronic Materials Management (EMM): monitoraggio e gestione inventario forniture mediche, farmaci e altri materiali (risorse di magazzino).

§ 1.3 Nuovi scenari di ICT in sanità

L'impiego dell'ICT in sanità, diventa oggi leva strategica per migliorare l'accesso ai servizi da parte dei cittadini/utenti nel contemporaneo sviluppo di, nuovi e precedentemente, impensabili prestazioni, che stanno cambiando le modalità di erogazione dei servizi per la cura e la salute delle persone.

L'esperienza di tante realtà regionali di eccellenza mostra chiaramente come un elevato livello d'informatizzazione, delle strutture sanitarie, possa contribuire in maniera significativa a migliori performance economiche associate all'esigenza di fornire ai cittadini servizi qualitativamente più elevati. Nel panorama nazionale, un'ulteriore risultato, è stato raggiunto con l'approvazione definitiva del "Decreto del Fare" (D.L. 21/6/2013 nr. 69) introducendo definitivamente il "Fascicolo Sanitario Elettronico", una piattaforma digitale dove saranno inserite le storie cliniche dei pazienti che saranno sempre on-line e fruibili in tempo reale da tutti i soggetti abilitati.

Le ragioni di opportunità connesse allo sviluppo di una gestione elettronica delle informazioni (es. conservazione digitale e FSE) sono numerose, come per esempio:

- Disponibilità di tutte le informazioni sanitarie con un click ed in ogni momento;
- Completezza informativa;
- Standardizzazione dei formati;
- Abbattimento dei costi di archiviazione e dei volumi;
- Possibilità di verifica degli accessi alle informazioni sanitarie;
- Automatizzazione dei sistemi di prenotazione delle visite, ritiro referti, con abbattimento dei costi e risparmio di tempo per il cittadino;
- Semplificazione del work-flow documentale in ambito clinico e amministrativo.

§ 1.4 L'Amministratore di Sistema

L'introduzione dell'ICT, in atto in Italia, in riferimento alle Risorse Umane coinvolte, ha evidenziato:

- che gli addetti appaiono oggi insufficienti rispetto ai compiti che li attendono nell'immediato futuro;
- occorre riconoscere adeguatamente le figure professionali relative l'ICT, promuovendone la formazione;
- è necessario promuovere e facilitare la formazione degli operatori sanitari sull'uso dei sistemi informativi e sulla gestione delle informazioni cliniche.

Tali riscontri evidenziano il "gap" di conoscenze e competenze non solo tra gli esperti di ICT all'interno delle strutture sanitarie, ma tra tutti i dipendenti comunque interessati all'utilizzo di queste nuove modalità e tecnologie di lavoro.

Per rispondere alle sfide che l'applicazione dell'ICT porta con sé sarà per questo necessario la riqualificazione del personale, soprattutto dei responsabili dei sistemi informativi ed informatici. Inoltre risulterà strategico, dal nostro punto di vista, la

nascita di figure di supporto alle attività degli operatori della sanità nell'utilizzo dei sistemi informatici.

Per il personale sanitario si tratta di un cambiamento culturale che comporta la necessità di svolgere le proprie mansioni attraverso l'ausilio di un supporto informatico e virtuale che sostituisce le operazioni manuali o in formato cartaceo[7].

L'impetuoso sviluppo tecnologico accompagnato dall'introduzione di nuove apparecchiature radiologiche, ad esempio, ha indotto un notevole incremento del numero di esami in radiologia eseguiti, amplificando le difficoltà dovute al trasporto e alla archiviazione dei risultati, contribuendo alla rapida informatizzazione della radiologia. La gestione di questa immensa mole di flussi informatici ha promosso lo sviluppo di un nuovo profilo professionale "***l'amministratore di sistema RIS/PACS"***: figura finalizzata alla gestione e manutenzione di un impianto di elaborazione o di sue componenti, o a quelle figure allo stesso equiparabili dal punto di vista dei rischi relativi alla protezione dei dati (come amministratori di base di dati, amministratori di rete e di apparati di sicurezza e gli amministratori di sistemi software complessi), che parla, contemporaneamente, il linguaggio del medico, del tecnico, del direttore sanitario e delle aziende fornitrici, rappresentando un ponte di collegamento tra esigenze tecniche e cliniche[8].

Alcune delle attività peculiari dell'amministratore di sistema sono a titolo di esempio: rispondere alle esigenze della direzione dell'ente gestito o ai quesiti degli utilizzatori del sistema stesso (utenti), risolvere problemi o guasti, gestire gli account utente, installare, configurare, migliorare ed aggiornare hardware o software, documentare tutte le

7 AA. VV. Ricerca: "L'impatto dell'informatizzazione sulle Aziende Sanitarie Lombarde e le relative implicazioni sulla formazione e addestramento degli operatori", Fondazione ISTUD per la cultura d'impresa e di gestione, Milano Dicembre 2003. http://www.istud.it/up_media/ricerche/equal_san.pdf ultimo accesso 12/08/2013

8 G. Di Nardo et altri, "Amministratore di Sistema RIS/PACS" in Management in Radiologia, ed Springer, Milano 2010, pag. 37

operazioni effettuate, pianificare e verificare la corretta esecuzione dei processi di salvataggio dei dati (backup/recovery) e gestire i supporti di memorizzazione.

L'amministratore di sistema nelle sue consuete attività è, in molti casi, concretamente responsabile di specifiche fasi lavorative che comportano elevate criticità, proprio rispetto alla protezione dei dati. Tali modalità, comportano un'effettiva capacità di azione su informazioni che vanno considerate a tutti gli effetti come trattamento di dati personali e/o sensibili.

In un Dipartimento di Diagnostica per Immagini e Radioterapia, per fare un esempio concreto, infatti, vi è la presenza, di quelli che il Garante per la Privacy definisce "software complessi" (Ris e Pacs), attraverso i quali si gestiscono una grandissima mole di dati sensibili, referti e immagini sottoposti a specifiche direttive di legge che ne regolamentano modalità e responsabilità di gestione ed archiviazione.

Per l'esercizio di tali attività è necessaria per questo una figura professionale con funzioni specialistiche, in possesso di uno specifico titolo. Il riconoscimento di tale figura, attualmente, in Italia, non è ancora ben definita e nelle realtà sanitarie l'attribuzione del ruolo di Amministratore di Sistema ad un TSRM si è insediata in maniera differente e variegata. Di fatti in alcuni casi l'amministratore di sistema non è un TSRM e, nei casi in cui lo è, non ha riconoscimento di progressione di carriera e/o coordinamento e non è in possesso di titoli professionali specifici. Inoltre nel 50% delle realtà sanitarie italiane il ruolo di Amministratore di Sistema, è affidata, con appositi contratti, a ditte esterne, spesso le stesse fornitrici della infrastruttura Hardware e Software dei sistemi Ris/Pacs, con personale con ridotte o assenti capacità/competenze cliniche.

La massima efficacia del RIS/PACS, che può essere considerata a pieno una Risorsa per l'intera organizzazione sanitaria, è ottenibile soltanto se gestito da un TSRM: il quale è l'unico operatore coinvolto nella creazione e prima gestione delle immagini cliniche.

§ 1.4.1 L'esperienza dell'A.U.S.L. Bologna

Presso l'Azienda USL di Bologna, una delle più grandi aziende sanitarie italiane (8700 dipendenti, 9 presidi ospedalieri, 74 poliambulatori, 53 sedi di consultori, 23 punti di continuità assistenziale), è stato raggiunto un importante riconoscimento nei confronti dei Tecnici Sanitari di Radiologia Medica formalizzando, da parte della Direzione dell'Azienda USL di Bologna, la "funzione di Amministratore di Sistema Ris/Pacs", riconoscendo come figura di elezione per lo svolgimento di tale funzioni il Profilo professionale di Tecnico Sanitario di Radiologia Medica. Tale riconoscimento qualifica ulteriormente la professione del Tecnico Sanitario di Radiologia Medica ed è stato ottenuto dall'impegnativo lavoro svolto da parte di diversi attori quali i TSRM (che già svolgevano questo ruolo nell'ambito dell'Azienda USL di Bologna) e l'università degli studi di Bologna attraverso la realizzazione anche di un Master Universitario che ne supportasse la formazione degli addetti ai lavori. Un intenso lavoro ha preceduto questa attribuzione per l'individuazione e definizione del ruolo e delle competenze dell'Amministratore di Sistema Ris/Pacs in cui ha avuto un ruolo essenziale la U.O.S. E-Care dell'Azienda USL di Bologna diretta dal Dott. Massimo Romanelli (TSRM).

§ 1.4.2 il processo di evoluzione professionale del TSRM e i master professionalizzanti.

In questi ultimi mesi il Ministero della Salute e le Regioni, in accordo con le rappresentanze professionali e sindacali, hanno individuato e stabilito quali dovranno essere, in generale, per ciascuna professione sanitaria, i master che potranno abilitare all'esercizio delle nuove competenze avanzate con l'introduzione delle specializzazioni previste dall'art. 6 della Legge 43/2006 che prevedeva, già, figure di professionisti sanitari in "possesso di master di primo livello per le funzioni specialistiche rilasciato dall'Università".

In un documento inviato alla Conferenza Stato-Regioni, per il recepimento e l'approvazione il 10/12/2012, sono state descritte le competenze che possono essere esercitate dal TSRM, in sette aree professionali e tra cui ha trovato affermazione l'area informatica, attraverso l'attivazione di un master in Amministratore di Sistema in Diagnostica per Immagini (ASIDI). Il TSRM ASIDI è il Professionista abilitato, in ambito universitario, alla gestione dei sistemi informativi in Area Radiologica; deve essere in possesso di specifiche competenze per curare la gestione di tecnologie informatiche in area radiologica; dei dati anagrafici e clinici con software e order entry, delle immagini prodotte, ottimizzandone la produzione e la trasmissione nel rispetto delle normative di sicurezza dei documenti informatici e della privacy. Si occupa, inoltre, dei processi formativi e di aggiornamento specifici del settore.

2. L'INFORMATICA DISTRIBUITA: LA RETE

§ 2.1 La rete informatica

Una delle caratteristiche rilevanti dell'Informazione archiviata in formato digitale è la sua grande capacità di movimento.

Durante il normale funzionamento di un PC, i bit, viaggiano incessantemente e velocemente tra le sue varie componenti interne attraverso canali detti BUS. Se opportunamente collegati, i computers, sfruttando la grande capacità di mobilità dei bit, possono scambiarsi dati e condividere risorse, distribuendo così il carico dell'elaborazione e dell'archiviazione delle informazioni.

Una "Rete di Computer" estendendo la "capacità di circolazione" dei bit può essere definita come un insieme di nodi o stazioni (non esclusivamente computer), o meglio di sistemi di elaborazione di informazione, dislocati in posti differenti e collegati tra loro mediante opportuni sistemi che consentono la trasmissione delle informazioni e/o la condivisione di risorse e servizi su aree geografiche ampie oppure di livello globale[9], realizzando notevoli vantaggi.

La rete è quindi un sistema che permette ad un certo numero di elementi indipendente (come computer, stampanti, plotter, fax, scanner, supporti di memorizzazione, masterizzatori, unità di back-up, etc. per citare alcuni esempi tra le risorse di comune utilizzo e diffusione) di raccogliere, gestire, comunicare, condividere (rendere accessibili) e trasferire risorse fisiche, software o dati e realizzare dei programmi

[9] R. Monaco, A. Lunghi, R. Panzica, P. Mattia, "Archivi integrati in Diagnostica per Immagini. Parte 1" in Annali degli Ospedali San Camillo Forlanini - Roma, vol. 8, num. 1 Gennaio – Marzo 2006, p. 50

modulati, i cui componenti sono eseguiti su computer diversi e collegati mediante la rete appunto.

§ 2.2 Architettura di una rete

Per realizzare la propria funzionalità di condivisione delle risorse, Hardware e Software, e dei dati, le Reti Informatiche si avvalgono di dispositivi di collegamento e trasmissione che sono composti, schematicamente, da:

- un *supporto fisico*, l'hardware, (detti anche "dispositivi passivo") che si differenzia in:
    - apparati di comunicazione o infrastruttura (così detto cablaggio strutturato),
    - dispositivi attivi, rappresentati da:
        - apparati di connessione per gli elaboratori (le interfacce di rete),
        - componenti per l'interconnessione e l'interfacciamento (apparati di rete),

  mediante i quali i computer vengono fisicamente collegati e lungo i quali supporti, viaggiano i segnali della comunicazione;
- un *supporto logico*, il software, rappresentato da programmi di gestione del collegamento e del traffico dati, tecnicamente denominati protocolli di comunicazione operanti su vari livelli di astrazione e che forniscono differenti servizi.
- da *Client o Stazioni di lavoro* (computer nella maggior parte dei casi) attraverso cui accedono gli utenti per utilizzare le "risorse" locali (dispositivi di periferia collegati direttamente e i software installati), le risorse informatiche condivise e

disponibili in rete (software di data base centralizzati), periferiche di rete (stampanti o scanner).

Il collegamento fisico tra le differenti entità della rete (server, client, periferiche di rete, dispositivi attivi, etc.) avviene attraverso una complessa infrastruttura che deve essere dimensionata sulla base delle esigenze dell'utente finale. Negli ambiti lavorativi o didattici le tipologie di reti informatiche più diffuse sono dette "LAN" (Local Area Network). Tale tipologia di rete si sviluppa genericamente a "stella gerarchica", soluzione che prevede molti collegamenti punto – punto connessi agli apparati centrali (hub o switch) e che garantisce grande flessibilità. Questa tipologia di collegamento è la più utilizzata in ambito Radiologico per la connessione del PACS (Picture Archiving and Communication System) con i singoli utenti e stazioni.

Nelle reti locali si distinguiamo due differenti tipologie di risorse: uno o più "Server" (un computer che mette a disposizione alcuni servizi come ad es. programmi, file, risorse hardware), da moltissimi "Client" che fanno richiesta dei servizi e che sono collegati, alla rete, mediante l'interconnessione ad un dispositivo (hub/switch) che smista il traffico nelle varie destinazioni, con la possibilità di aggiungere o rimuovere i dispositivi senza condizionare la funzionalità della rete.

§ 2.3 Il cablaggio strutturato

Con il termine "cablaggio" s'intende l'infrastruttura, generalmente passiva (cavi, connettori, prese terminali, pannelli di permutazione, cavi di raccordo, etc.) che realizza la rete, permettendo il collegamento tra gli utenti e le risorse, attraverso il trasporto dei diversi segnali in modo flessibile, affidabile e veloce.

La progettazione e realizzazione/istallazione di una Rete Informatica, che deve essere predisposta nelle opere civili alla pari dell'impianto elettrico, idraulico e tecnologico,

segue alcune norme di riferimento che contengono requisiti di prestazione, sicurezza e idoneità all'installazione. La rispondenza ai requisiti di standardizzazione internazionale permette di gestire l'infrastruttura in maniera aperta multi-prodotto e multi-marca, garantendo prestazioni prestabilite e rappresentando una soluzione definitiva ed universale.

Il sistema di cablaggio ha lo scopo di ripartire il segnale dati ai vari utenti della rete raggiungendo tutti i locali ed ogni ufficio. Ciò avviene in comunicazione tra l'armadio di permutazione centralizzato con i ripartitori collocati sui vari piani dell'edificio e una distribuzione che porta, a sua volta, il segnale, da ogni armadio di piano alle singole prese utente. Dal punto di vista gerarchico si distingue:

- ***il cablaggio verticale***, definito anche cablaggio o dorsale di edificio, realizzato solitamente mediante cavi in fibra ottica, identifica il cavo principale e le sue derivazioni agli armadi di piano. Connette i vari rami di cablaggio orizzontale e normalmente si sviluppa in verticale in quanto collega i distributori di ogni piano dell'edificio.
- ***Il cablaggio orizzontale*** è la connessione realizzata da ciascuna presa utente, delle cosiddette Work Area, al distributore di piano. Viene anche definito come cablaggio di piano, perché in un edificio a più piani, connette, normalmente tutti gli utenti di un singolo piano.

§ 2.4 Elementi costituenti una rete RIS/PACS

La rete informatica appena descritta è lo strumento utilizzato per "collegare" gli utenti alle risorse, compiendo in questo la centralizzazione dei servizi per agevolare lo scambio dei dati.

L'ambito della "Diagnostica per Immagini" è caratterizzato dalla presenza di Sistemi Informativi dedicati, talvolta fisicamente distinti oppure tecnologicamente integrati, ed informatizzati e rappresentanti dal:

- RIS (Radiology Information System), con il compito di assicurare la gestione complessiva del flusso di lavoro e dei dati generali;
- PACS (Picture Archive Communication System), che ha la funzione di provvedere alla generazione, visualizzazione e distribuzione delle immagini, sia ai fini della refertazione che dell'archiviazione.[10]

La funzione di questi sistemi è:

- Acquisizione, in formato digitale delle immagini fornite dalle diverse apparecchiature diagnostiche e dei dati ad esse associate;
- Elaborazione ed archiviazione di informazioni relative ai diversi momenti della storia clinica/anamnestica del paziente;
- Condivisione in rete di tutte le informazioni di utilità clinica ed amministrativa.

Questi sistemi, sono un esempio di risorse, che nell'ambito sanitario, sfruttano i vantaggi offerti da una Rete Informatica, realizzata all'interno di una struttura ospedaliera e che di seguito analizzeremo.

Un sistema RIS/PACS consente un'efficiente gestione ed archiviazione delle immagini digitali e si integra nella struttura informatica di un'Azienda Ospedaliera, in cui la rete locale connette i diversi poli.

La Rete Informatica, infatti, è l'infrastruttura utilizzata dai sistemi RIS/PACS per comunicare tra le loro componenti e con il Sistema Informativo Ospedaliero (HIS) con l'obiettivo di permettere l'accesso ai dati clinici prodotti dalla Diagnostica per Immagini

[10] P. Berti, D. Ciuffi, G. Messina, "La Digitaliazzione in Radiodiagnostica. Aspetti Operativi e gestionali". Mondo Sanitario 1-2/2011, p.1

(immagini e referti) sia nel luogo di esecuzione dell'esame (in Radiologia, per la stessa refertazione, stampa delle immagini significative, produzione del CD paziente contenente tutte le immagini acquisite) sia nel luogo in cui avviene la diagnosi clinica, ottimizzando per questo la collaborazione che avviene tra Radiologo, clinico, paziente/utente e le diverse strutture sanitarie, eventualmente coinvolte, come ad esempio la distribuzione a distanza delle immagini/referto (internet o cd/dvd) per la consultazione.

Il sistema PACS si basa su architettura E.O.L. (Everthing On Line) che consente di mantenere "in linea" su RAID le immagini mediamente prodotte nel corso dell'anno da un dipartimento di diagnostica per immagini, in quanto statisticamente l'accesso a immagini acquisite da oltre un anno si è dimostrato raro.

Un PACS non è soltanto un sostituto del classico archivio cartaceo, si tratta di una struttura più complessa con un architettura ben precisa, in quanto possiede delle unità di acquisizione (es. CR, DR, CT, MR, ECO, PET, NM), delle unità di memorizzazione/sicurezza, di consultazione/elaborazione, di stampa ed infine si appoggia ad una solida infrastruttura di rete che compendia un database.

Una volta che l'immagine è stata "prodotta" il sistema di acquisizione, mediante software dedicati, permette alcune operazioni sulle immagini stesse (come ad es. annotazioni, apposizione di lettera di lato, modifica del contrasto secondo filtri, collimazione dei bordi, scelta del layout di stampa).

Dopo aver ottimizzato, secondo i criteri e le possibilità del software a disposizione, lo studio viene confermato e viene rilasciato al PACS, mediante un programma di autorouting o alla stampa su pellicola/CD, o ad entrambe.

Una volta che il PACS riceve lo studio, provvede all'archiviazione in base alle scelte compiute dall'Azienda e nel rispetto dei requisiti legali imposti dalla legge.

Per la memorizzazione delle immagini il sistema PACS sfrutta un'architettura di tipo gerarchico o HMS (Hierarchical Storage Management), che possiede la seguente struttura:

- On line: a recupero rapido, non necessita di intervento umano né robotico (RAID)
- Near Line: richiede computer-controlled Robot per l'accesso più rapido possibile ad una grande quantità di dati (solitamente residenti su juke box a dischi ottici UDO);
- Off Line: prevista per l'archiviazione legale con requisito principale della "non riscrivibilità" e mantenimento dei dati (compressione Lossy), mediante tecnologia UDO (Ultra Density Optical Disk da 30Gb, 60Gb o 120Gb per disco, oppure DVD).

La caratteristica fondamentale di un disco RAID è la possibilità di ricostruire i dati che si trovano su un disco danneggiato. In informatica un RAID (Redundant Array of Indipendent Disk), insieme ridondante di dischi indipendenti, è uno standard informatico che utilizza più dischi in parallelo, per condividere o replicare le informazioni, tipicamente utilizzato nei server e/o archivi dati. Il sistema RAID permette di combinare un insieme di dischi in una sola unità logica che il Sistema Operativo gestisce come un unico volume[11]. Questo standard permette di aumentare l'integrità dei dati, infatti, i dati che vengono immagazzinati non devono essere persi per nessuno motivo e quindi si ricorrere a questo tipo di sistema per la generazione di informazioni ridondanti.

[11] Wikipedia: RAID http://it.wikipedia.org/wiki/RAID ultimo accesso 2 settembre 2013

Nonostante i progressi nella conservazione e nelle tecnologie di trasmissione, la compressione delle immagini è indispensabile, riducendo non solo le esigenze di storage (o archiviazione) ma anche i tempi di trasmissione dei dati. La compressione delle immagini può avvenire secondo una delle seguenti modalità:

- Lossless: compressione senza degradazione dell'immagine. Viene normalmente utilizzata su tutte le immagini prima dell'esecuzione della refertazione, dal momento che tale compressione non cambia l'immagine né in termine di pixel né nelle dimensioni. Tecnica preferibile in quanto permette di recuperare un'immagine identica all'originale con un fattore 1:1,5 – 1:2.
- Lossy: parte dell'informazione viene persa con la compressione e permette di ottenere quindi fattori di compressione maggiori e superiori a 10. In molti casi fornisce immagini praticamente equivalenti all'originale. Solitamente viene effettuata dopo la diagnosi. In generale però proprio per la natura di alterazione dell'immagine, si tende ad evitare questo tipo di compressione delle immagini, preferendo lo spostamento di immagini e dati, non più utilizzati dopo un certo tempo, negli archivi ottici, meno costosi e a lungo termine.

L'aumento delle tecnologie digitali ha permesso di consegnare ai pazienti una documentazione su supporti CD/DVD e non più su comuni pellicole fotografiche. In questo modo, il paziente, può conservare tutto il materiale clinico/diagnostico con più praticità e, nel caso, gli venga richiesto di fornire la documentazione degli esami precedenti, trasportarlo più facilmente. Inoltre i files contenuti nei supporti digitali hanno la possibilità di essere visualizzati su qualsiasi PC (portabilità).

Per realizzare le funzioni tipiche descritte sono necessari componenti hardware e software che possono essere classificati come segue:

- Server applicativi e database per la gestione dei RIS
- Server applicativi e database per la gestione del PACS
- Imaging system, dispositivi di acquisizione delle immagini provenienti dalle differenti modalità diagnostiche (computer di acquisizione o workstation di refertazione);
- Archive system, dispositivi di archiviazione delle immagini diagnostiche su supporti digitali;
- Dispositivi di visualizzazione, elaborazione e stampa delle immagini, rappresentati da workstation di consultazione e dalle loro periferiche;
- Applicativi software
- Infrastruttura di rete

§ 2.5 Patologie di una rete di computer

La comunicazione diretta da computer a computer, non più limitata ad ambiti circoscritti e protetti, ma estesa, anche grazie ad Internet, su scala globale, aumenta esponenzialmente i rischi per la sicurezza derivanti dall'esecuzione di programmi nocivi o altre applicazioni pericolose[12]. I "Malware" o programmi nocivi sono creati deliberatamente e specificamente per usi fraudolenti o illegali e la loro esecuzione può causare danni di diverso tipo, come ad esempio: furto o distruzione di informazioni, blocco o grave intralcio al funzionamento di singoli computer o di intere reti.

I programmi nocivi tradizionalmente vengono classificati in macro-categorie, distinguendoli ad esempio in virus, macrovirus, worm, trojan, ma si è recentemente assistito alla comparsa di una nuova generazione di programmi nocivi in grado di

[12] AA.VV. "Introduzione alla medicina in rete", Corso FAD a cura della Fondazione IRCCS CA' GRANDA Ospedale Maggiore Policlinico di Milano e ecmcampus.it, 2013 tratto da www.ecmcampus.it (previa registrazione) ultimo aggiornamento 2 settembre 2013, cap. 7 pag. 51

sfruttare sinergicamente tutte le caratteristiche delle singole categorie elencate come esempio.

L'interesse degli odierni progettisti di malware, non più generalmente Haker isolati, ad intrufolarsi nei computer di migliaia di utenti è sempre meno riconducibile al semplice gusto del "danno per il danno" e sempre più finalizzato a carpire informazioni economicamente rilevanti[13].

I danni, anche economici, derivanti dalla diffusione di malware sono numerosi, come ad esempio:

- Asservimento di un computer al controllo di terzi e suo sfruttamento per attività illegali;
- Furto di dati confidenziali;
- Blocco o rallentamento dei servizi;
- Alterazione o cancellazione dei dati;
- Malfunzionamenti vari.

Mentre i virus classici causavano tipologie di danno più facilmente circoscrivibili, i nuovi programmi nocivi multipurpose, basati su "cavalli di troia" esibiscono una gamma tale di attività da rendere assai più problematica la disinfezione: essi possono ricevere ed inviare file, eseguirli, visualizzare messaggi, accedere a pagine web, scaricare ed installare programmi e riavviare il computer infetto.

I virus si diffondono prevalentemente attraverso lo scambio di programmi o documenti tra computer diversi. Lo scambio può avvenire anche attraverso documenti infetti

[13] AA.VV. "Introduzione alla medicina in rete", Corso FAD a cura della Fondazione IRCCS CA' GRANDA Ospedale Maggiore Policlinico di Milano e ecmcampus.it, 2013 tratto da www.ecmcampus.it (previa registrazione) ultimo aggiornamento 2 settembre 2013, cap. 7 pag. 51

pubblicati in rete o sull'intranet o spediti come allegati di messaggi e-mail (qualsiasi messaggio di posta elettronica può essere vettore di software nocivo).

Alcuni sintomi comuni che possono indicare che il nostro sistema è infetto sono[14]:

- Messaggi o immagini inconsuete sul monitor;
- Suoni o musiche insolite che si ripresentano alternativamente;
- Il sistema ha meno memoria libera di quanta dovrebbe;
- Un disco o un volume hanno cambiato nome;
- Programmi o file che all'improvviso non si trovano più;
- Vengono creati file o programmi nuovi e sconosciuti;
- Alcuni dei nostri file sono rovinati e all'improvviso non funzionano più come dovrebbero;
- File (soprattutto archivi) che crescono in modo spropositato;
- Crash di sistema.

Nel caso di Worm o Trojan, invece, i sintomi sono generalmente costituiti dal rallentamento del sistema e dalla presenza di traffico internet quando non dovrebbe essercene. Nella logica della sicurezza informatica è più conveniente spendere tempo e denaro per tenere una minaccia fuori dal sistema, perché se un virus dovesse entrare nel pc, la sua rimozione a posteriori non potrebbe rimediare ad un furto di dati, oppure ad una infezione così estesa da necessitare una formattazione del sistema. Questo implica anche tutta una serie di conseguenze come i costi del

[14] AA.VV. "Introduzione alla medicina in rete", Corso FAD a cura della Fondazione IRCCS CA' GRANDA Ospedale Maggiore Policlinico di Milano e ecmcampus.it, 2013 tratto da www.ecmcampus.it (previa registrazione) ultimo aggiornamento 2 settembre 2013, cap. 7 pag. 57

lavoro dei tecnici informatici, la perdita di dati essenziali e le eventuali riconfigurazioni[15].

Naturalmente nessuna misura di sicurezza, e non solo in campo informatico, offre assoluta protezione, ed una certa percentuale di rischio è inevitabile. Metodi, tecniche e strumenti per la sicurezza, uniti a comportamenti consapevoli devono essere adottati per diminuire tale percentuale di rischio ad un livello accettabile.

Infatti il mondo sanitario è fortemente vulnerabile a questo tipo di attacchi, per la relativa poca dimestichezza con le procedure di sicurezza informatica del personale che molto spesso non è formato rispetto a queste problematiche e non ha una adeguata "cultura della security"[16].

Questo genere di attacchi, finora descritti, nella maggior parte dei casi, sono relativi al comportamento, alle abitudini, il più delle volte alla disponibilità, alla non conoscenza e alla non malizia dell'utente di cui si vogliono carpire, a sua insaputa, informazioni sulle sue identità digitali (come ad es. password, codici bancari).

Per proteggersi da questa tipologia di patologie è utile e necessario:

- Aggiornare il sistema operativo e il browser, che offrono solitamente già alcune funzioni di sicurezza;
- Attivare il Firewall (del sistema operativo) oppure installare un software di Firewall efficace e relative opzioni di configurazione. Il Firewall consiste generalmente in un pc posto sul Gateway sul quale è applicato un programma che filtra i messaggi in arrivo e protegge il computer o la rete da

15 R. Grassi in: appendice F "Cenni sulla sicurezza informativa", tratto da: AA.VV. "Elementi di informatica in Diagnostica per Immagini", ed. Springer, Milano 2010, p. 391

16 E. Frumento "Le minacce informatiche e l'evoluzione dei sistemi informatici ospedalieri" (Cap. 1) tratto da AA. VV. "La sicurezza nei sistemi informativi sanitari", ed. Edisef, Roma 2010 p. 23

accessi non autorizzati, garantendo per questo la privacy e l'integrità dei dati;

- Installare software antivirus e antispyware, scansionando con regolarità il pc e tutti gli eventuali messaggi di email ricevuti o file trasferiti mediante supporti esterni soprattutto da persone sconosciute;
- Non aprire file eseguibili di provenienza incerta o comunque scansionarli con i software antivirus;
- Non effettuare transizioni finanziarie, a meno che non siano effettuate con collegamenti e con modalità protette;
- Proteggere con password i pc o i dischi fissi;
- In casi di informazioni sensibili usare la crittografia;
- Fare copie di backup;
- Informarsi con continuità sul tema.

3. CORRETTO UTILIZZO DELLA RETE INFORMATICA

§ 3.1 Utilizzo di una rete informatica in Diagnostica per Immagini

Alla fine dell'acquisizione dei dati e dopo successive elaborazioni e trattamenti da parte del medico specialistica radiologo o medico nucleare o del tecnico saitario di radiologia medica, il quale ultimo agisce comunque su delega dello specialista stesso, si ottiene una serie di file, di formato DICOM, contenente i risultati. Questi possono essere delle semplici immagini (Istances), dei risultati numerici (Evidence Documents) o dei filmanti (Multiframe Istances). In ogni caso non si tratta di dati ottenuti da interpretazione diagnostica/clinica.

Queste evidenze informatiche vengono trasferite sul sistema PACS (Picture Archiving and Communication System) ove vengono sottoposte a procedimento di archiviazione con l'apposizione di una gerarchia di riferimenti univoci (generalmente generati dalle apparecchiature stesse) identificanti la singola immagine, la serie e lo studio di appartenenza, quest'ultimo costituito da insiemi di serie relative al medesimo paziente che concorrono alla produzione del responso diagnostico complessivo. Tutte le immagini dello studio diventano quindi disponibili per la refertazione da parte del medico e, una volta effettuata, messa in lista per essere sottoposta, insieme al referto sottoscritto con firma digitale o qualificata, a procedimento di conservazione.

In generale le eventuali correzioni di errori nell'associazione tra i dati paziente e le immagini del paziente possono essere eseguite dal personale autorizzato, mediante apposite procedure codificate, approvate a livello aziendale e condivise dal responsabile dell'U.O. di Diagnostica per Immagini, che permettano la tracciatura dei vari passaggi. Al termine delle modifiche il richiedente delle stesse deve essere sempre avvertito, con

apposita e tempestiva segnalazione, circa l'avvenuta correzione. Tutte le operazioni descritte devono essere archiviate su un opportuno sistema informatico di radiologia (RIS). Le immagini inviate al PACS non devono mai essere cancellate: errori di associazioni di immagini e paziente devono avvenire per spostamento di immagini.

Dal punto di vista della conservazione è invece necessario che gli studi refertati, che hanno visto la modifica di anche una sola delle immagini in essi contenuti, siano sottoposti, mediante apposite procedure codificate, a una nuova conservazione, in modo da garantire la disponibilità nel tempo dello studio modificato e collocare temporalmente in modo opponibile a terzi l'avvenuta modifica.

Nella gestione della documentazione totalmente elettronica occorre individuare un momento per il "perfezionamento" in cui il documento smette di essere una semplice "bozza" e diventa a tutti gli effetti un "originale" e coincide con il momento in cui l'autore, dopo aver visionato a video il contenuto del documento e averne corretto gli eventuali errori ne dà una conferma definitiva, utilizzando la firma elettronica (paternità del documento rendendolo nel contempo immodificabile) e la marcatura temporale (datare in modo certo), per dare oggettività a questa conferma (garanzie di autenticità della sottoscrizione, immodificabilità del documento, certezza della data).

La procedura necessaria, per garantire nel tempo la validità legale di un documento informatico, viene definita "***conservazione sostitutiva***", consentendo evidenti risparmi sui costi di stampa, di stoccaggio e di archiviazione.

Per una adeguata gestione dei documenti di Diagnostica per Immagini dematerializzati, è auspicabile l'implementazione di una serie di misure tecniche atte ad assicurare la correttezza delle procedure e il controllo dei processi, misure che sono già oggetto di

norme, come quelle sulla privacy, e che devono quindi essere predisposte per la tutela sia dei pazienti che degli operatori.

Si auspica inoltre che ogni aspetto della gestione venga monitorato da appositi meccanismi informatici, tali da poter definire con precisione, per ogni operazione effettuata sui sistemi, orario, tipo e autore di ciascuna operazione compiuta. Ciò permette di risalire con precisione alla responsabilità individuale di comportamenti ed azioni di rilevanza non solo amministrativa, ma anche clinica e penale.

Requisiti minimi di sicurezza che devono essere adottati nella gestione informatica sono:

- Avere un sistema di autenticazione informatica,
- Possedere un sistema di autorizzazione per profili
- Avere copie di backup

L'articolazione del flusso di lavoro che avviene all'interno di una struttura ospedaliera che dispone di sistemi informatici integranti, durante l'esecuzione di un esame radiologico, prevede il susseguirsi di numerosi elementi. Il processo finale di refertazione dell'esame radiologico e dunque della Conservazione Sostitutiva della documentazione (con l'eventuale consegna del referto stesso) parte dalla prenotazione o comunque dal primo approccio alla struttura da parte del paziente per arrivare alla chiusura amministrativa delle attività effettuate, e prevede le seguenti fasi, informatizzate o meno, secondo il contesto ospedaliero: Prenotazione, Accettazione, Esecuzione, Refertazione, Firma e Stampa, Archiviazione, Consegna, Ricerca e Statistica, Rendicondazione.

§ 3.2 I documenti informatici e dematerializzazione in Radiologia. Il Quadro normativo di riferimento della documentazione radiologica.

Archiviare e conservare tutta la documentazione, in particolare quella radiologica prodotta sta diventando sempre più necessario per via degli innumerevoli vantaggi da questa offerta, permettendo:

- da un punto di vista clinico, il rapido accesso a tutti gli approfondimenti diagnostici precedenti;
- da un punto di vista organizzativo, con la razionalizzazione e l'ottimizzazione di risorse umane e tecnologiche;
- da un punto di vista medico-legale, con la totale disponibilità nella struttura erogatrice della documentazione originale immodificabile.

La normativa oggi applicabile alla documentazione sanitaria in formato elettronico è regolata dal Decreto Legislativo del 7 marzo 2005 nr. 82 cd. "Codice dell'amministrazione digitale" (CAD), modificato dal D. Lgs. del 30/11/2010 nr. 253[17], in cui vengono definite e regolate la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale, utilizzando le tecnologie dell'informazione e della comunicazione più appropiate, all'interno della Pubblica Amministrazione e nei rapporti tra amministrazioni e privati.

Per la Diagnostica per Immagini, riconosciuta come Unità Operativa maggiormente informatizzata all'interno delle strutture sanitarie italiane, in considerazione della loro rilevanza strategica nei processi di diagnosi e cura, si è resa necessaria l'emanazione di un ulteriore documento, rappresentato dalle "Linee Guida per la dematerializzazione della documentazione clinica in Diagnostica per Immagini. Normativa e Prassi."

17 Tratto da: http://www.funzionepubblica.gov.it/lazione-del-ministro/linee-guida-siti-web-pa/indice/cap1-destinatari-e-normativa/principi-della-amministrazione-digitale.aspx (ultimo accesso 19 settembre 2013)

(Conferenza Stato-Regioni , marzo 2012)[18]. L'obiettivo perseguito, nella stesura di questo importante documento, è stato quello di massimizzare l'affidabilità e la sicurezza per quanto attiene la produzione e gestione della documentazione sanitaria in formato digitale e supportare fattivamente l'interscambio informativo, l'interoperabilità e l'integrazione funzionale tra i diversi soggetti preposti alla cura dei cittadini.

Inoltre, tutte le attività del work-flow radiologico, compresa la produzione delle immagini, rientrano a pieno titolo, in quelle previste nel D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali (art. 4, comma 1, lett. a). Infatti il "trattamento" va inteso come "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione di dati, anche se non registrati in una banca dati"[19]. Pertanto tutti i procedimenti di dematerializzazione, in ambito sanitario, ed in particolare nella Diagnostica per Immagini, riguardano dati personali idonei a rivelare lo stato di salute del paziente, per il trattamento dei quali è assolutamente necessario prestare la massima cura, ottemperando con precisione alle disposizioni del Decreto.

In ambito della Diagnostica per Immagini la documentazione prodotta è diversificata in resoconti ed iconografia (secondo quando individuato dall'art. 3 del D.M. 14/2/1997 e art. 111, comma 10, del D. Lgs. n. 230 del 17/3/1995):

[18] tratto da: http://www.statoregioni.it/DettaglioDoc.asp?IDDoc=35770&IdProv=10549&tipodoc=2&CONF=CSR (ultimo accesso 19 settembre 2013)

[19] art. 4, comma 1, lett. a, D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali" tratto da http://www.camera.it/parlam/leggi/deleghe/03196dl.htm (ultimo accesso 19 settembre 2013)

- I documenti radiologici e/o di medicina nucleare, consistono nelle immagini quali risultato dell'esecuzione dell'indagine diagnostica, puro eseito degli esami eseguiti mediante la strumentazione;
- I resoconti (radiologici o di medicina nucleare) rappresentano i referti stilati dal medico specialista radiologo o medico nucleare. Il referto (resoconto radiologico) è l'atto obbligatoriamente redatto in forma scritta, con il quale lo specialista dell'Area Radiologica (Medico Radiologo o Medico Nucleare) formula l'interpretazione delle immagini ottenute dagli esami diagnostici, tenendo conto del quadro clinico e dell'anamnesi del paziente.

Le radiografie, o più genericamente le immagini, non rivestono il carattere di atti ufficiali, ma sono i dati su cui si deve basare la refertazione diagnostica del medico specialista radiologo o del medico nucleare, e sono paragonabili ai preparati istologici e citologici[20]. La documentazione è pertanto un prodotto privo di interpretazione o valutazione clinica da parte dello specialistica, trattandosi di una pura lettura di un dato analitico. Per queste motivazioni, si ritiene, che tranne che in casi di oggettiva emergenza e/o regolati da appositi protocolli, le immagini ed il referto devono essere messe in disponibilità contestualmente e subito dopo la firma digitale del referto.

Analogamente a quanto accade per i referti le modalità di gestione delle immagini diagnostiche (rappresentazioni iconografiche) è normata dal D.M. 14/2/1997, che descrive le specifiche fasi di acquisizione, archiviazione e disponibilità delle stesse immagini. In particolare l'art. 4, comma 1, afferma che, "ove la documentazione iconografica non venga consegnata al paziente, questa deve essere custodita con le modalità di gestione in grado di garantirne la disponibilità. Vanno quindi archiviate, e

[20] Circolare Ministero Sanità n. 62 del 19/12/1986, n. 900.2/AG 464/260 "Periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura".

sottoposte successivamente al processo di conservazione a termini di legislazione vigente, tutte le immagini digitali in formato DICOM prodotte dalle aparecchiture di diagnostica per immagini di tutta la struttura sanitaria ovvero realizzate a qualsiasi titolo nelle proprie U.O.

Ai fini della conservazione, la normativa di riferimento (D. Lgs. 230/95, D.M. 14/2/1997, Circolare Min. Sanità n. 61/86 e D.P.R. 14/2/1997) non fa differenza in alcun modo fra la documentazione analogica e quella digitale e per questo motivo, avviene secondo quanto indicato schematicamente nella succesiva tabella (Tabella 1 - obblighi di conservazione dei documenti radiologici).

Referto Analogico		
	Tempo	responsabile
Interno	Illimitato	Direzione Sanitaria
Esterno	Non previsto dalle norme nazionali. Possibilità di previsione da parte di norme regionali	Paziente o UO di Diagnostica per Immagini
Referto Informatico		
Interno	Illimitato	Responsabile Conservazione
Esterno	Non previsto dalle norme nazionali. Possibilità di previsione da parte di norme regionali. Sia auspica illimitato	Paziente o UO di Diagnostica per Immagini
Immagini Analogiche		
Interno	10 anni	UO di Diagnostica per Immagini o Paziente
Esterno	Non previsto	paziente
Immagini Digitali		
Interno	10 anni	UO di Diagnostica per Immagini fino all'atto della conservazione; successivamente il Responsabile della Conservazione
Esterno	10 anni	
Referto strutturato		
Interno	Illimitato	UO di Diagnostica per Immagini fino all'atto della conservazione; successivamente il Responsabile della Conservazione
Esterno	Illimitato	

Tabella 2 - obblighi di conservazione dei documenti radiologici[21]

21 Fonte: "Linee Guida per la Dematerializzazione della Documentazione Clinica in Diagnostica per Immagini. Normativa e Prassi" (3/2012)

§ 3.3 La sicurezza informatica in ambito sanitario

Il concetto di sicurezza informatica è collegata a quel complesso di accorgimenti tecnici ed organizzativi che mira a presidiare la riservatezza, la confidenzialità, l'integrità e la disponibilità dei dati informatici. Ogni volta che su un paziente vengono creati, aggiornati, modificati, copiati, trasferiti, archiviati o distrutti, dati sensibili, la sicurezza di queste stesse informazioni deve essere salvaguardata.

Un sistema informatico, viene definito, sicuro, quando le informazioni riservate, non sono disponibili, a chi non è autorizzato, ma disponibili, nella loro integrità e autenticità originaria, per chi ne ha pieno diritto, garantendo, inoltre, ad ogni paziente, il rispetto della privacy.

Anche l'improvviso black-out o il cattivo funzionamento, oltre al deficit di sicurezza dei sistemi di elaborazione e trasmissione dei dati informatici, può generare ingenti danni, esponendo le strutture erogatrici di prestazione sanitaria, che fanno uso di reti informatiche (come la diagnostica per immagini), a notevoli rischi, anche di natura economica.

Sulla base dell'esperienza maturata in altri contesti, come quello bancario, si può affermare che vi sono numerose soluzioni utili per garantire la sicurezza delle informazioni, ma è importante rilevare che, il mondo della sanità, rischia di trovarsi impreparato alla difesa dell'asset che gestisce, in quanto le soluzioni tecnologiche esistenti o sono poco orientate alla sicurezza o se lo sono (come ad es. HL7 e Dicom) non sono mai state testate da attacchi reali, diretti, appositamente scritti o progettati per l'ambiente sanitario.

A tal riguardo esistono oggi numerosi livelli di protezione, che possono differenziarsi in:

- Fisici, che non consentono agli estranei l'accesso ai dati e che preservano l'hardware da eventuali danni dovuti ad es. ad incendi, cortocircuiti o allagamenti;
- Logici, basati sul controllo dell'accesso, che consente di porre un filtro all'accesso indiscriminato ai dati da parte di chiunque.

§ 3.3.1 Protezione fisica di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento dei dati sono protetti e dotati di:

- Dispositivi antincendio (estintori, o altro);
- Stabilizzatore di tensione dell'alimentazione elettrica;
- Impianto di condizionamento

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli immobili ed i locali nei quali avviene il trattamento devono essere protetti da sistemi di allarme antintrusione e sistemi di chiusura a chiave degli ambienti il cui utilizzo ed accesso è regolato secondo procedure definite dai diversi responsabili del trattamento stesso.

La custodia e l'archiviazione di atti, documenti e supporti, di terminali e pc, che trattano dati sensibili avviene mediante l'utilizzo di cassetti ed armadi con serratura, locali chiudibili a chiave, nei quali devono essere riposti i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal proprio posto di lavoro, anche temporaneamente.

§ 3.3.2 Misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori, e qualunque altro dispositivo elettronico o comunque automatizzato) si devono adottare le seguenti misure:

- Realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinchè ad ogni strumento elettronico possa accedere solo chi è autorizzato;
- Realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle mansioni lavorative;
- Realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus);
- Prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti removibili (floppy disk, dischi zip, CD, DVD ed etc.), nei quali sono contenuti dati personali.

§ 3.3.3 Salvaguardia dei dati

Le grandi quantità di dati trattati e soprattutto la particolare natura degli stessi, ci spingono ad adottare non solo sistemi di sicurezza degli accessi ma anche sistemi di backup che consentono di salvaguardare l'intero patrimonio informativo.

I dati possono essere classificati in base alla loro natura e per ognuna di queste categorie vi sono logiche distinte di salvataggio su supporti di memorizzazione,

anche di natura diversa del supporto scelto (disco magnetico), oltre che in destinazioni fisicamente diverse[22]. È per questo preferibile l'impiego di personale dedicato e di attrezzature in grado di robotizzare le procedure di salvataggio dei dati programmandole nei diversi giorni della settimana e sfruttando orari poco critici. Il backup di una base di dati avviene normalmente nelle ore di fermo delle attività o, soprattutto nel caso di aree sanitarie, nelle ore di minor affluenza di lavoro e quindi quando il data base è sollecitato da poche transazioni, effettuando un lavoro di configurazione e soprattutto di controllo su tutte le operazioni affinchè riescano in maniera corretta e che non ci siano anomalie, attuando se necessario politiche e tecniche di archiviazione distinte. A tal proposito devono essere effettuati periodicamente dei test di ripristino dei sistemi per verificare ed avere consapevolezza dei tempi di ogni singola fase,

§ 3.4 Riservatezza ed Autorizzazioni

I dati contenuti all'interno del sistema informatico possono essere utilizzati da diversi attori:

- da chi fornisce assistenza (medico e professioni sanitarie coinvolte);
- da chi utilizza l'assistenza stessa (pazienti e loro familiari);
- da chi gestisce l'assistenza (amministrazione e direzione sanitari, a livello locale, regionale e nazionale);

La responsabilità in merito a quali informazioni vedere od utilizzare è sempre responsabilità dell'operatore, che deve limitarsi alla visualizzazione dei dati necessari

[22] G. Guerrieri "L'Esperienza dell'Azienda Ospedaliera San Giovanni Addolorata di Roma" (Cap. 10) tratto da "La sicurezza nei sistemi informativi sanitari" (A cura di F. Di Resta, B. Ferraris di Celle), Roma 2010, ed. Edisef., p. 213

per svolgere la propria funzione assistenziale rispetto allo specifico caso.[23], in quanto vi sono numerose situazioni in cui un operatore sanitario può, anche inavvertitamente, commettere una violazione di legge.

Per questo sono stati sviluppati dei meccanismi, tra di loro correlati, di autenticazione, di autorizzazione, di auditing, che permettono di tutelare la confidenzialità delle informazioni, impedendo l'accesso a di chi non è autorizzato.

L'autenticazione. È l'operazione mediante la quale si verifica che qualcuno sia chi dice di essere, proteggendo il sistema, non solo da accessi non autorizzati, ma anche garantire gli utenti legittimi, se operano correttamente ed in buona fede. L'utilizzatore può essere identificato, secondo una sorta di scala di affidabilità dei meccanismi di autenticazione, grazie a qualcosa di cui è a conoscenza, che è in suo possesso o che l'utilizzatore è.

L'autorizzazione. Operazione con la quale si verifica se qualcuno ha il permesso di accedere ad una risorsa o di eseguire un operazione. In base all'identità accertata dell'utilizzatore, il sistema, può negargli l'accesso, consentirgli l'accesso esclusivamente con determinate modalità, permettergli di eseguire soltanto alcune operazioni.

L'auditing. È un attività generalmente svolta a posteriori, mirata a valutare un'organizzazione, sistema, processo o prodotto. Con riferimento al controllo degli accessi ed alle implicazioni pratiche per coloro che utilizzano il sistema informatico, l'auditing consente di accertare validità ed affidabilità di un'informazione. A tal fine viene utilizzato il cosiddetto audit trail (tracciatura o tracciamento), ovvero l'insieme

[23] AA.VV. "Sistemi informativi sanitari e trattamento informatizzato dei dati clinici", Corso FAD a cura della Fondazione IRCCS CA' GRANDA Ospedale Maggiore Policlinico di Milano e ecmcampus.it, 2013 tratto da www.ecmcampus.it (previa registrazione) ultimo aggiornamento 2 settembre 2013, cap. 7 pag. 56.

delle registrazione delle operazioni svolte all'interno del sistema (chi ha fatto cosa e quando l'ha fatto)[24].

§ 3.5 Strumenti per garantire la sicurezza nei sistemi informativi sanitari

Gli aspetti correlati alla sicurezza in Diagnostica per Immagini sono di crescente rilievo nella pratica assistenziale e fanno riferimento alla sicurezza dei comportamenti professionali in Radiologia e nell'utilizzo dei sistemi RIS e PACS necessitando di specifiche attività, attenzione ed integrazione multiprofessionale, estendendo agli strumenti di gestione del rischio anche l'ambito della diagnostica per immagini.

Nell'attività sanitaria l'Evento Sentinella (ES) è definito come un evento avverso di particolare gravità, potenzialmente evitabile, che può comportare morte o grave danno al paziente e che determina una perdita di fiducia dei cittadini nel confronti del servizio sanitario. Il verificarsi di un solo caso è sufficiente per dare luogo ad un indagine conoscitiva diretta ad accertare sevi abbiano contribuito fattori eliminabili o riducibili e per attuare le adeguate misure correttive da parte dell'organizzazione[25].

Il principale obiettivo della gestione del rischio in Diagnostica per Immagini consiste nel ridurre e, dove possibile, eliminare l'eventualità che si verifichino eventi causativi di un danno per il paziente. Tale obiettivo è perseguibile attraverso l'apprendimento degli errori e il monitoraggio degli incidenti più significativi e critici e dei quasi incidenti (near miss).

---

24 AA.VV. "Sistemi informativi sanitari e trattamento informatizzato dei dati clinici", Corso FAD a cura della Fondazione IRCCS CA' GRANDA Ospedale Maggiore Policlinico di Milano e ecmcampus.it, 2013 tratto da www.ecmcampus.it (previa registrazione) ultimo aggiornamento 2 settembre 2013, cap. 8 pag. 76-77.

25 Ministero della Salute, Protocollo Sperimentale di Monitoraggio degli Eventi Sentinella. I Rapporto periodo settembre 2005 – febbraio 2007 http://www.apelpediatri.it/Leggi/Governo%20Clinico,%20Sicurezza%20dei%20pazienti%20C_17_pubblicazioni_676_allegato.pdf (ultimo accesso 20 settembre 2013)

A Bologna nel settembre del 2007 si è verificato un avvenimento che ha tutte le caratteristiche di un evento sentinella e che ci sembra opportuno ricordare.

La gestione di un numero cospicuo di immagini e di anagrafiche, la necessità di produrre, leggere, interpretare e trasmettere le informazioni in modo sicure ed appropriato, fanno si che il sistema di gestione del rischio diventa parte integrante di ogni fase del processo radiologico con l'obiettivo della riduzione degli eventi critici da cui potrebbe derivare un danno al paziente.

§ 3.5.1 Il caso di bologna

Una paziente di 54 anni il 5 luglio del 2007 (paziente 1) si recava al pronto soccorso del Policlinico S. Orsola – Malpighi di Bologna lamentando una lombosciatalgia. L'esecuzione di un'ecografia dimostrava una lieve dilatazione dell'uretere di sinistra e la presenza di angiomiolipoma renale di 13mm, dato confermato in una seconda ecografia ripetuta in ambiente privato successivamente. Il 13 agosto 2007, su richiesta del medico curante e con il quesito diagnostico di sospetta neoplasia renale, veniva sottoposta presso la Radiologia del Policlinico ad un uro-TC. Al termine dell'indagine venne inviato al server del PACS l'intero studio. Il Tecnico Sanitario di Radiologia Medica (TSRM) in servizio nel turno TC era il Sig. X e il medico Radiologo di turno era il dott. A. Il giorno successivo, il 14 agosto era sottoposta ad Uro-TC una paziente di 86 anni (paziente 2), omonima per cognome rispetto alla paziente 1, affetta da neoplasia del segmento pre-vescicale dell'uretere sinistro con conseguente idro-ureteronefrosi di III-IV grado. Il TSRM in turno era il medesimo del giorno precedente, il Sig. X, e il Medico Radiologo era invece il dott. B.

1° evento critico. Al termine dello studio vennero inviate le immagini al doppio Server PACS, ma attribuite erroneamente alla paziente 1 del giorno precedente (1° evento critico), nominativo che compariva ancora in elenco nella worklist della consolle della TC, nella riga adiacente a quella della paziente 2. Tale errore fu subito corretto dal TSRM X: sulla consolle della TC i dati anagrafici e l'ID paziente del paziente 1 furono corretti come paziente 2 e l'intero studio venne inviato normalmente al PACS. Poco dopo il TSRM intervenne sui due Server (del PACS e del WEB) con l'intento di rimuovere le immagini errate del caso di paziente 2, associate ed inviate per errore come paziente 1.

2° evento critico Dal server del PACS (consultabile dalla Radiologia e che permette di inviare le immagini ai robot per la masterizzazione dei CD) fu invece cancellata (2° momento critico) la sequenza di 1585 immagini corrispondente al vero esame del paziente 1 (acquisite il 13 agosto) e rimasero solo le 1641 immagini del paziente 2 del 14 agosto ma scorrettamente attribuite al paziente 1.

Sul server WEB, che invia le immagini a tutto l'ospedale e consultabile solo dai reparti clinici, venne invece effettuata correttamente la cancellazione della sequenza sbagliata e restarono disponibili solo le immagini della paziente 1.

3° evento critico Il normale comportamento operativo di allora non prevedeva l'allerta del Radiologo di riferimento da parte del TSRM X che avvenuta la correzione delle registrazioni relative alla paziente 1 non avvertì il dott. A (3° momento critico). Il TSRM X era abilitato alla funzione di correzione, svolte altre volte prima di allora, ignaro dell'errore.

Lo studio TC della paziente 2, regolarmente archiviato nel PACS, venne refertato dal dr. B il 17/8/2007 descrivendo un quadro di vistosa idroureteronefrosi sinistra di III grado per stenosi neoplastica dell'uretere distale aggettivante la vescica, suggerendo un completamento con esame citoscopico.

4° evento critico Lo studio della paziente 1 (immagini sbagliate della paziente 2 con dati anagrafici corretti e con la sola discrepanza di data sulle immagini) veniva refertato dal dott. A il 17/8/2007 e convalidato il 20/8/2007 (4° momento critico) descrivendo un quadro di vistosa idroureteronefrosi sinistra di III grado per stenosi neoplastica dell'uretere distale aggettivante in vescica, consigliano di effettuare una cisto-ureteroscopia di approfondimento diagnostico del quadro clinico. Le immagini di entrambe le ecografie eseguite precedentemente e discordanti con il quadro TC non erano visualizzabili per confronto nel PACS della Radiologia.

In data 17/8/2007 il dott. A consultò il dott. B, considerandolo più esperto in uro-radiologia, sul caso del paziente 1, ma senza che il secondo riconoscesse che il caso possedeva le medesime caratteristiche di quello da lui di recente refertato (paziente 2). Al momento del ritiro del referto venne anche consegnato al paziente 1 un CD contenente le relative immagini (errate).

Il paziente 1 fu sottoposta a cisto-ureteroscopia dagli stessi urologi che in seguito la operarono: in considerazione della macroscopica negatività del quadro cistoscopico, l'urologo esecutore ritenne di non dover effettuare l'ureteroscopia.

La discordanza tra i reperti TC (positivi), cistoscopici ed ecografici (negativi), indusse l'urologo ad inviare un collabortore in Radiologia per verificare le immagini contenute nel CD e quindi per richiedere una consulenza radiologica.

5° evento critico Per la turnazione dei radiologi, tale consulenza fu fornita in via estermporanea da in terzo Radiologi in quel momento in servizio, il dott. C (5° momento critico) che verifica la presenza di patologia e la discordanza tra i reperti TC e quelli delle altre metodiche diagnostiche. L'urologo poneva comunque l'indicazione ad intervento di nefroureterectomia, senza procedere ad ulteriori accertamenti diagnostici. Risulta, dagli accertamenti in corso, che prima dell'intervento, fossero state comunque visualizzate le immagini contenute nel WEB, e quindi corrette, della paziente 1, nel computer della sala operatoria.

6° evento critico Durante l'intervento eseguito per via laparoscopica (la scelta di questa modalità operatoria ha rappresentato il 6° momento critico), dopo avere clampato e sezionato i vasi renali, l'urologo si rese conto delle discrepanza del quadro renale di tipo non patologico, con assente dilatazione dell'uretere (che invece appariva nelle immagini TC contenute nel CD, unica metodica valutata in fase preoperatoria) e ricercò sul web il caso, visualizzando per la prima volta le immagini corrette e rinvenendo una condizione totalmente diversa da quella presente sul CD, con una stostnziale normalità dei reperti renali. Data la fase avanzata dell'intervento, questo fu comunque terminato effettuando la nefrectomia del rene sano. Il giorno successivo la Direzione dell'Unità Operativa informava la paziente 1 ed i familiari, illustrando quanto accaduto. La mattina ancora seguente la paziente 1 decedeva per embolia polmonare dopo alcuni episodi ipotensivi manifestati durante la notte precedente[26].

[26] informazioni tratte da: "Il Radiologo" nr. 2/08 pag. 26-33, reperito via web all'indirizzo http://www.tsrm-pu.org/news/doc_news/il_caso_di_Bologna.pdf ultimo accesso 20 settembre 2013

Preliminari
1) prenotazione CUP di esame inappropriato carente giustificazione preliminare
2) elevati carichi di lavoro TC (18/20 pazienti/turno da 6h e 20 min.)
3) organico medico ridotto per ferie (12-19 agosto)
Nel fatto
1) omonimia del Cognome delle pazienti
2) persistenza nella worklist dei pazienti inseriti ed effettuati nei 3 giorni precedenti
3) cancellazione 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) referto radiologico stilato dopo 4 gg. Dall'esame sulle immagini scambiate
6) successivo consulto estermporaneo tra Clinico e un terzo radiologo
7) mancata consultazione del caso sul Web-Server, preliminarmente all'intervento, da parte dell'urologo
8) modalità di intervento chirurgico (laparoscopia vs. chirurgia tradizionale)
Terapeutici
Mancata somministrazione terapia antiaggregante in pz. Operata a rischio di trombo embolitico per via dell'obesità

Tabella 3 eventi critici caso di Bologna

§ 3.5.2 Sistema di Gestione della Sicurezza delle Informazioni: la ISO 27001:2005

La sicurezza delle cure è un diritto del paziente e requisito imprescindibile per un'organizzazione sanitaria, dal momento che incide sui risultati in termini economici e di immagine (perdita di fiducia). La gestione del rischio diventa per questo parte integrande della sicurezza e si esplica nelle attività cliniche, gestionali ed amministrative per indentificare, valutare e ridurre il rischio di eventi avversi e di danni per il paziente, per gli operatori e i visitatori, nonché il rischio di perdite per l'organizzazione sanitaria. Nell'ambito dei servizi informativi tutto questo presuppone un approccio organizzativo (linee guida) per garantire un giusto livello di sicurezza soprattutto per quanto riguarda lo scambio di dati e informazioni tra le varie modalità dei reparti ospedalieri e più in particolare di un reparto di radiologia.

Per realizzare questo scopo si può adottare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), di cui lo **Standard UNI CEI ISO/IEC 27001:2006** rappresenta un modello. La **UNI CEI ISO/IEC 27001:2006** è una norma internazionale che definisce i

requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese **Information Security Management System**), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.

L'obiettivo dell'ISO 27001:2005 è quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (SGSI) finalizzato ad una corretta gestione dei dati sensibili dell'azienda. L'impostazione dello standard ISO/IEC 27001 è coerente con quella del Sistema di Gestione per la Qualità ISO 9001:2000 ed il Risk management[27].

Lo standard, progettato per assicurare la selezione di controlli per la sicurezza, adeguati e proporzionati, in grado di proteggere i beni informativi, adotta l'approccio per processi, per stabilire, attuare, condurre, monitorare, riesaminare, mantenere attivo e migliorare il SGSI di un'organizzazione. Tale approccio, secondo il modello "Plan-Do-Check-Act", permette di individuare e comprendere i requisiti per la sicurezza delle informazioni di un'organizzazione e della necessità di stabilire politiche ed obiettivi per la sicurezza delle informazioni, di attuare ed eseguire controlli per gestire i rischi collegati alla sicurezza delle informazioni di un'organizzazione, monitorare e riesaminare le prestazioni e l'efficacia del SGSI e del miglioramento continuo sulla base di misurazioni oggettive compiute.

Di fondamentale importanza è l'Appendice A che contiene **133 "controlli"** (o contromisure) a cui, l'organizzazione che intende applicare la norma, deve

[27] tratto da: Wikipedia http://it.wikipedia.org/wiki/ISO/IEC_27001

attenersi. Essi vanno dalla politica e l'organizzazione per la sicurezza alla gestione dei beni alla sicurezza delle risorse umane, dalla sicurezza fisica e ambientale alla gestione delle comunicazioni e dell'operativo, dal controllo degli accessi fisici e logici alla gestione del monitoraggio e trattamento degli incidenti (relativi alla sicurezza delle informazioni), dalla gestione della Business Continuity al rispetto normativo.

Per attuare tale politica gestionale in sistemi informatici di un reparto di radiologia sarà, ad esempio necessario:

- Condividere un modello di analisi e verifica di follow-up basato sugli standard esistenti, (con controlli periodici per valutare lo stato di aggiornamento delle apparecchiature hardware e software);
- Uniformare i database
- Minimizzazione dei rischi relativi alla gestione dei dati paziente nell'ambito dell'utilizzo dei sistemi ris/pacs installati: ottimizzando la configurazione dei sistemi ris/pacs installati, redigere e implementare procedure/istruzioni operative, effettuare periodicamente attività di follow-up, formazione continua degli addetti di reparto;
- Verificare a monitor la correttezza dei dati anagrafici e la data di esecuzione dell'indagine, facendosi carico delle modifiche di tutte le aree nelle quali figurano dati errati, evitando quindi la generazione di errori a catena;
- Attuazione di processi di identificazione del paziente con il riconoscimento anagrafico del paziente durante l'accettazione e attraverso la predisposizione di check-list di verifica paziente, di sito, lato e tipologia in caso di interventi chirurgici

Una nuova versione ISO/IEC 270011, si stima, dovrebbe essere pubblicata tra ottobre e novembre 2013 secondo nuove direttive definite dalla ISO, e con una nuova strutturazione, tesa all'allineamento di tutte le norme dei sistemi di gestione ad una medesima organizzazione dei contenuti avviando così di fatto un progetto di integrabilità tra esse da parte di un organizzazione.

§ 3.5.3 La Certificazione E.C.D.L. Healt nella sicurezza informatica in sanità

L'ambiente sanitario si è trovato costretto ad affrontare frequentemente con ritardo il problema dell'informatizzazione, soprattutto perché si è da sempre scontrata, con un tasso di alfabetizzazione informatica molto basso con gravi ricadute non soltanto in termini clinico/sanitari ma anche socio/economici.

La Certificazione E.C.D.L. Health nasce con la finalità di fornire agli operatori del comparto sanitario un framework di riferimento sulle "conoscenze necessarie per utilizzare in modo consapevole le applicazioni ICT che trattano informazioni dei Pazienti"[28], valorizzando il fattore umano nella considerazione che anche il Sistema Informativo Sanitario più sofisticato in termini Hardware e Software è perfettamente inutile se non usato da un personale adeguatamente formato.

Siccome la sicurezza informatica è in realtà sicurezza dell'informazione, il fattore umano rappresenta la vera strategia che può e deve essere gestito, nel senso nobile del termine, grazie ad opportuni programmi di formazione e addestramento. La certificazione ECDL Health in tal senso rappresenta un

[28] http://www.aicanet.it/aica/ecdl-health

formidabile strumento per fornire all'operatore sanitario il riferimento ampio e completo, per la cultura dell'informazione sanitaria[29].

Il motore della Certificazione ECDL Health, come per qualsiasi altra Certificazione, è naturalmente il Syllabus, ossia il "contenitore", in formato ragionato, di tutti gli argomenti di cui s'interessa la Certificazione stessa. Il Syllabus si articola in quattro sezioni e in relativi punti di approfondimento. La proposta del Syllabus 1.1, attualmente in vigore dal 2010, si articola in: 1) concetti, 3) compiti assistenziali, 3) abilità dell'utente, 4) norme e procedure, ulteriormente organizzate in temi ed argomenti.

Nella certificazione ECDL Health il tema della sicurezza informatica o della sicurezza dell'informazione è assolutamente pervasivo, perché vale anche e soprattutto come orientamento culturale, in quanto, si parla, non soltanto di sicurezza del dato, ma soprattutto della sua protezione.

Il principale punto di riferimento legislativo, ovviamente per quanto riguarda la Legislazione italiana, della Certificazione ECDL Health è il D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali) ed il suo Allegato B (Disciplinare Tecnico in materia di misure minime di sicurezza).

Dato che il fattore più importante per l'implementazione della sicurezza dell'informazione in sanità è la risorsa umana, opportunamente formata e addestrata, e dato che la certificazione ECDL Health individua proprio nella sicurezza la principale problematica d'interesse, sembra naturale eleggere la Certificazione a fondamentale veicolo di sviluppo della cultura informatica sanitaria in generale e alla sicurezza informatica in particolare.

[29] G. Festa, A. Teti "Il Contributo della Certicazione ECDL Health alla sicurezza dell'informazione in sanità" (Cap. 9) tratto da "La sicurezza nei sistemi informativi sanitari" (A cura di F. Di Resta, B. Ferraris di Celle), Roma 2010, ed. Edisef., pp. 185 e successive

CONCLUSIONI

L'evoluzione dei servizi sanitari accompagnata dall'evoluzione tecnologica permetterà di favorire la collaborazione tra le strutture e gli operatori, cercando di "muovere" le informazioni e non le persone, facendo leva su un driver fondamentale del mondo sanitario: la cosiddetta "Equity": offrendo a tutti la possibilità di accedere, con pari opportunità, ai servizi migliori ed evoluti dell'intero sistema sanitario.

La sfida, già in atto, consiste nel completare e rendere realmente permanente nella sanità, l'adozione di standard per la condivisione dei dati e l'integrazione dei vari servizi informativi.

Le nuove tecnologie mediche e i nuovi "modi di catturare" e utilizzare le informazioni medicali sono i due principali aspetti che si prevede rivoluzioneranno la sanità nel prossimo futuro, senza dimenticare, però che ad una maggiore informatizzazione dei processi ed una distribuzione dei dati più complessa, si associano anche crescenti problemi di sicurezza, direttamente proporzionali al valore dei dati (Asset) ed alla complessità della rete che li elabora (sistema informativo ospedaliero).

La rapida diffusione dei Sistemi Informativi ed informatici, come ad esempio i sistemi RIS/PACS nei dipartimenti di Diagnostica per Immagini, hanno profondamente cambiato il tradizionale workflow, rendendo sempre di maggiore importanza, dal punto di vista strategico, le iniziative formative e scientifiche per l'addestramento del personale, al fine della ottimale gestione ed implementazione di questi nuovi sistemi.

La gestione dei sistemi informatici dovrà prevedere un'adeguata organizzazione con l'individuazione di figure professionali "nuove", come l'Amministratore di Sistema, con competenze specifiche nel campo informatico, radiologico, normativo-legislativo e nella gestione dell'immagine radiografica digitale.

BIBLIOGRAFIA

- P. Berti, D. Ciuffi, G. Messina "La digitalizzazione in radiodiagnostica. Aspetti operativi e gestionali", da Mondo Sanitario nr. 1-2 2011;
- Disposizioni urgenti in materia di semplificazione e di sviluppo (D. L. n. 5 del 9/2/12);
- Disposizioni in Materia di Sanità Digitale (L. n. 35 del 4/4/2012);
- C. Calamandrei, C. Orlandi "La Dirigenza infermieristica. Manuale per la formazione dell'infermiere con funzioni manageriali", ed. Mc-Graw-Hill, Milano 2009 (III edizione);
- G. Donna. S. Nieddu. M. Bianco "Management Sanitario. Modelli e strumenti per gli operatori delle aziende sanitarie", ed. Centro Scientifico Editore, Torino 2003;
- F. Mazzuccato "Anatomia Radiologica. Tecnica e metedologia in radiodiagnostica", ed. Piccin Padova 2009;
- AA.VV. Ricerca: "L'impatto dell'informatizzazione sulle Aziende Sanitarie Lombarde e le relative implicazioni sulla formazione e addestramento degli operatori", Fondazione ISTUD per la cultura d'impresa e di gestione, Milano Dicembre 2003;
- L. Bolognini, E. Pellino "Cloud in Sanità: Vademecum essenziale sulla tutela della privacy. Manuale sui principi, sulle caratteristiche, sulle specifiche normative in materia di protezione dei dati da applicare in Italia all'erogazione di servizi sanitari con tecnologia cloud computing", ed. FederSanità-Anci & Istituto Italiano Privacy Roma 2013;
- AA. VV. "Management in Radiologia", ed. Spinger, Milano 2010
- AA.VV. "Dalla carta al digitale" Italia Oggi serie speciale nr. 7 anno 19 del 11/2/2009, ed. Italia Oggi Erienne S.R.L., Milano 2009;
- AA.VV. "Archivi integrati in Diagnostica per Immagini. Parte 1", in Annali degli ospedali San Camillo Forlanini – Roma, Vol. 8, num. 1 Gennaio-Marzo 2006;
- AA.VV. "introduzione alla medicina in rete", Corso FAD, a cura della Fondazione IRCCS CA' GRANDA Ospedale Maggiore Policlinico di Milano ed Ecmcampus.it, 2013;
- AA. VV. "La sicurezza nei sistemi informativi sanitari", ed. Edisef, Roma 2010;
- AA.VV. "Elementi di informatica in Diagnostica per Immagini", ed. Spinger, Milano 2010;
- AA. VV. "Sistemi informativi sanitari e trattamento informatizzato dei dati clinici", Atti Corso FAD, a cura della Fondazione IRCCS CA' GRANDA Ospedale Maggiore Policlinico di Milano ed Ecmcampus.it, 2013;
- D. Lgs. 196/2003, Codice in materia di protezione dei dati personali;

- Circolare Ministero Sanità n. 62 del 19/12/1986 n. 900.2/AG 464/260 "Periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura";
- Linee Guida per la Dematerializzazione della Documentazione Clinica in Diagnostica per Immagini. Normativa e prassi (3/2012);
- O. Nicastro, "Sicurezza in Diagnostica per Immagini", atti seminario di primavera 2011, organizzato da Agenzia Sanitaria e Sociale Regionale e Regione Emilia Romagna, Bologna 2012;
- AA.VV. "Il Radiologo", nr. 2/08