CARTELLA CLINICA ELETTRONICA OSPEDALIERA

Indicazioni per un progetto sostenibile

A cura di

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

In collaborazione con

ANORC

Associazione Nazionale Operatori e Responsabili della Conservazione

Clusit

Associazione Italiana per la Sicurezza Informatica

CARTELLA CLINICA ELETTRONICA OSPEDALIERA

Indicazioni per un progetto sostenibile

A cura di

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

In collaborazione con

ANORC

Associazione Nazionale Operatori e Responsabili della Conservazione

Clusit

Associazione Italiana per la Sicurezza Informatica

CARTELLA CLINICA ELETTRONICA OSPEDALIERA

Indicazioni per un progetto sostenibile

Hanno partecipato al progetto

PARTECIPANTI AL GRUPPO DI LAVORO

Andaloro Antonino - AO Valtellina - Valchiavenna - antonino.andaloro@aovv.it

Bagnasco Manuela - Elco - manuela.bagnasco@elco.it

Balconi Daniela - Intersystems - daniela.balconi@intersystems.com

Barbariga Silvia - Medas - silvia.barbariga@medas-solutions.it

Barbon Fabio - Exprivia - fabio.barbon@exprivia.it

Benevenuti Carlo - Anorc - carlo.benvenuti@syncromed.it

Borile Giovanni - AO Padova - giovanni.borile@sanita.padova.it

Buzziol Sandro - Dedalus - sandro.buzziol@dedalus.eu

Caccia Claudio - MultiMedica Spa - claudio.caccia@multimedica.it

Capra Gianfranco - Dedalus - gianfranco.capra@dedalus.eu

Cardin Franco - Anorc - franco.cardin@alice.it

Cuciniello Maria - CeRGAS-Bocconi - maria.cucciniello@sdabocconi.it

Dallaturca Marco - Anorc - m.dallaturca@bmplaneta.it

De Nardi Paolo - AO Padova - paolo.denardi@sanita.padova.it

Di Vita Elena - Elco - elena.divita@elco.it

Del Ghianda Fabio - Estav Nord-Ovest - fabio.delghianda@estav-nordovest.toscana.it

Fabiano Roberto - eUtile - roberto.fabiano@e-utile.it

Faiella Daniela - Exprivia - daniela.faiella@exprivia.it

Farinelli Chiara - AO Cuneo - farinelli.mc@ospedale.cuneo.it

Ferrara Fabio - Anorc - fabio.ferrara@2fconsulting.net

Ferraris Cristian - Assolombarda - Cristian.Ferraris@assolombarda.it

Ferri Umberto - Medas - umberto.ferri@medas-solutions.it

Foglia Luigi - Anorc - luigifoglia@studiolegalelisi.it

Fornaro Lino - Anorc - lifo@take.it

Franco Giuseppe - S.Raffaele Cefalù - giuseppe.franco@hsrgiglio.it

Fregonara Mario - AO Novara - m.fregonaramedici@maggioreosp.novara.it

Gabbi Paolo - Adobe - paolo.gabbi@katamail.com

Gallo Domenico - Ag. Region. Sanitaria Liguria - domenico.gallo@regione.liguria.it

Garrisi Graziano - Anorc - grazianogarrisi@studiolegalelisi.it

Gasparetto Alessio - Ulss 18 Rovigo - gasparetto.alessio@azisanrovigo.it

Gatti Alfredo - Cionet - alfredo.gatti@cionet.com

Giovanardi Davide - Microsoft - davide.giovanardi@microsoft.com

Giraudo Roberto - CSI Piemonte - roberto.giraudo@csi.it

Giraudo Marco - CSI Piemonte - marco.giraudo@csi.it

Gomezortiz Olga - eUtile - olga.gomezortiz@e-utile.it

Iantorno Carlo - Microsoft - carlo.iantorno@microsoft.com

Leschiera Raffaello - Engineering - raffaello.leschiera@eng.it

Libonati Andrea - Deadalus - andrea.libonati@dedalus.eu

Lipodio Davide - Engineering - davide.lipodio@eng.it

Lisi Andrea - Anorc - andrealisi@studiolegalelisi.it, direzione@anorc.it

Lovotti Roberta - Sysline - roberta.lovotti@sysline.it

Luciani Alberto - Engineering - alberto.luciani@eng.it

Mangia Massimo - Federsanità - mangia@federsanita.it

Malandra Aura - CSI Piemonte - aura.malandra@csi.it

Nasi Greta - CeRGAS-Bocconi - greta.nasi@sdabocconi.it

Orsi Giorgio - AO Sacco - orsi.giorgio@hsacco.it

Pocobelli Barbara - Estav Nord-Ovest - barbara.pocobelli@estav-nordovest.toscana.it

Parravicini Renzo - Sysline - renzo.parravicini@sysline.it

Pedranzini Giovanni - Pgmd Consulting - pedranzini@pgmdconsulting.com

Perini Corrado - Intersystems - corrado.perini@intersystems.com

Piazza Tommaso - Ismett - tpiazza@ISMETT.edu

Pilon Sofia - Gruppo Don Gnocchi - spilon@dongnocchi.it

Pignatale Francesco - Intel - francesco.pignatale@intel.com

Pinelli Nicola - Fiaso - pinelli@fiaso.it

Ramaccini Simone - Medas - simone.ramaccini@medas-solutions.it

Repaci Guido - Aused - guido.repaci@virgilio.it

Ronchi Alberto - Istituto Auxologico - a.ronchi@auxologico.it

Rosati Maurizio - CSI Piemonte - maurizio.rosati@csi.it

Saccardo Ivo - Dedalus - ivo.saccardo@dedalus.eu

Sandini Bruno - Ulss Vicenza - bruno.sandini@ulssvicenza.it

Santambrogio Fabio - Fuji - fabiosantambrogio@fujimed.it

Sartori Lucio - Ulss Vicenza - lucio.sartori@ulssvicenza.it

Savino Nicola - Anorc - nicola.savino@seensolution.com

Serratore Carmela - Noemalife - cserratore@noemalife.com

Simonelli Ettore - Engineering - ettore.simonelli@eng.it

Telmon Claudio - Clusit - claudio@telmon.org

Tibaldi Raffaella - Noemalife - rtibaldi@noemalife.com

Vallega Alessandro - Oracle-Clusit - alessandro.vallega@oracle.com

Valcher Paolo - Microsoft - paolo.valcher@microsoft.com

Vella Claudio - Aisis - claudio.vella@polimi.it

Vitali Marco - Elco - marco.vitali@elco.it

Zanella Gianpaolo - GPI - gianpaolo.zanella@gpi.it

GLOSSARIO

ADT	**Sistema di gestione delle attività di Accettazione amministrativa, Dimissione, Trasferimento**
CCC	**Cartella Clinica Cartacea**
CCE	**Cartella Clinica Elettronica**
CIO	**Chief Information Officer**
CPOE	**Computerized Physician Order Entry**
CUP	**Sistema di gestione delle prenotazioni di prestazioni diagnostiche o specialistiche**
DCE	**Documento Clinico Elettronico**
EHR	**Electronic Health Record**
EMR	**Electronic Medical Record**
EPR	**Electronic Patient Record**
FEA	**Firma Elettronica Avanzata**
FSE	**Fascicolo Sanitario Elettronico**
ICT	**Information Communication Technology**
JCI	**Joint Commission International**
OTP	**One Time Password**
PEC	**Posta Elettronica Certificata**
PHR	**Personal Health Record**
PSN	**Piano Sanitario Nazionale**
PS	**Sistema di gestione delle attività di Pronto Soccorso**
RIA	**Rich Internet Applications**
SDO	**Scheda Dimissione Ospedaliera**
SIO	**Sistema Informativo Ospedaliero**
VDI	**Virtual Desktop Infrastructure**

SOMMARIO

PREMESSA

Il tema della cartella clinica elettronica ospedaliera riveste oggi un'importanza rilevante in quanto rappresenta una concreta possibilità di qualificare i livelli di servizio erogati dalle aziende sanitarie in un'ottica di razionalizzazione dei processi organizzativi e delle risorse ad essi connesse.

La possibilità di fornire servizi maggiormente efficienti ai cittadini e nel contempo di poter disporre, a fronte di un unico investimento, di informazioni utili sia per la gestione dei processi di qualità/rischio clinico (tracking del processo) sia di cost accounting appare un obiettivo raggiungibile grazie a un utilizzo strategico e intensivo delle tecnologie informatiche.

Data l'importanza dell'argomento, pur consapevoli dei limiti insiti in un approccio che non può coinvolgere tutti gli stakeholder che esprimono interessi su un progetto di CCE ospedaliera (clinici, infermieri, esperti di qualità, cittadini…) Aisis, in collaborazione con Anorc e Clusit, ha ritenuto opportuno proporre un contributo, attraverso la predisposizione di questo documento di linee guida, che possa favorire l'attivazione e la gestione di progetti di CCE intesi come la gestione del percorso diagnostico-terapeutico-assistenziale attraverso un utilizzo pervasivo della tecnologia informatica che nel corso del documento verrà chiamato cartella clinica elettronica ospedaliera.

Considerando che la realizzazione di questi progetti complessi richiede la capacità di una visione multidisciplinare, Aisis ha ritenuto necessario che la predisposizione di tale documento fosse proposta e condivisa con diversi attori coinvolti in tale processo: CIO, esperti di sicurezza rappresentati da Clusit, esperti di Conservazione Sostitutiva rappresentati da Anorc, mondo delle imprese e mondo universitario.

L'obiettivo del documento consiste nel fornire indicazioni basate sulla "sostenibilità" delle soluzioni proposte: non si tratta di trovare le migliori soluzioni possibili sotto il profilo tecnologico ma soluzioni, strumenti e metodologie che possano consentire a questi progetti di essere sostenibili intendendo con questo termine la probabilità oggettiva che questi progetti vengano avviati e completati in tempi e costi certi.

Nel primo capitolo del documento vengono introdotte alcune tematiche di contesto relative all'adozione della CCE in ambito ospedaliero; nel secondo capitolo vengono affrontate le funzionalità minime che un sistema di CCE deve garantire nell'ottica della copertura dei processi clinico-assistenziali; nel terzo capitolo si approfondiscono le tematiche di sicurezza, privacy, firma elettronica e conservazione sostitutiva; nel quarto capitolo vengono suggerite metodologie e strumenti per un "governance" di questi complessi e articolati progetti che richiedono modifiche culturali, organizzative, tecnologiche e di change management.

È quindi con grande piacere che Aisis, Anorc e Clusit presentano questo documento nella speranza di fornire indicazioni utili all'attivazione di progetti di realizzazione della Cartella Clinica Elettronica in ambito ospedaliero.

Dr. Claudio Caccia - Presidente di Aisis - Associazione Italiana Sistemi Informativi in Sanità

Dr. Paolo Giudice - Segretario Generale di Clusit - Associazione Italiana Sicurezza Informatica

Avv. Andrea Lisi - Presidente di Anorc - Associazione Nazionale Operatori e Responsabili della Conservazione

Milano, 23 novembre 2012

INTRODUZIONE

Il documento che verrà presentato nei prossimi capitoli ha l'obiettivo di fornire indicazioni per l'attivazione di sistemi di cartella clinica elettronica in ambito ospedaliero. Trattandosi di una tematica particolarmente complessa e articolata, appare necessario circoscrivere in modo chiaro il perimetro funzionale di cosa si intende per "cartella clinica elettronica ospedaliera" preso atto che tale termine si presta ad alcune ambiguità dovute a una normativa che non sempre, nel corso del tempo, ha colto i significativi mutamenti sia di tipo organizzativo-gestionali avvenuti nelle aziende ospedaliere sia delle nuove regole e norme inerenti la sicurezza informatica, la privacy, le norme di tipo archivistico e di conservazione sostitutiva.

In tale contesto, con specifico riferimento alla Linee Guida sul Fascicolo Sanitario Elettronico del Ministero della Salute, alle medesime linee guida del Garante per la protezione dei dati personali, alle linee guida Joint Commission International vers. 2011 e ad alcuni documenti regionali, nel documento che segue per "cartella clinica elettronica ospedaliera" si intendono **i processi del percorso diagnostico-terapeutico-assistenziale ospedaliero supportati dalle tecnologie informatiche**.

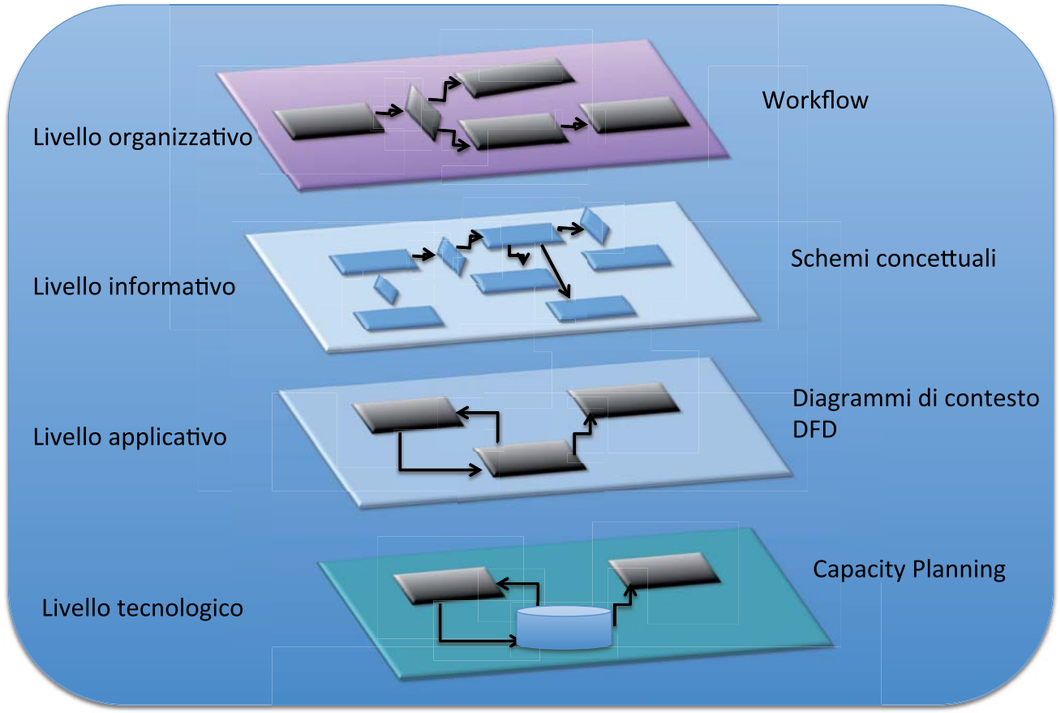
Preso atto che nella prassi e nella normativa italiana si sono adottate terminologie che non coincidono con le definizioni adottate a livello internazionale nello schema seguente viene proposta, a fini di massima chiarezza espositiva, una sintesi di tali differenze da cui scaturiranno, nella trattazione dei vari capitoli del documento, indicazioni relative ai contenuti, alla sicurezza, all'utilizzo di strumenti di firma elettronica, alla conservazione digitale, alla gestione di questi complessi progetti. Nell'area evidenziata sono sintetizzati i contenuti della CCE in ambito ospedaliero.

	Electronic Medical Record	Electronic Patient Record	Electronic Health Record	Personal Health Record
Definizione Internazionale definizione secondo Medical Record Institute	Un'architettura orientata alla gestione integrata dei flussi informativi dell'area clinico-sanitaria di una singola azienda con l'obiettivo di assicurare un governo complessivo del percorso diagnostico-terapeutico-assistenziale	Sono architetture basate sul sistema EMR ma hanno un ambito di operatività più ampio, ovvero sono soluzioni condivise da professionisti che operano in strutture diverse distribuite sul territorio	L'insieme dei dati e dei documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti un cittadino. Ha un orizzonte temporale che copre l'intera vita del cittadino. Il cittadino può accedere al EHR e inserire informazioni circa il proprio stato di salute al fine di garantire un processo di continuità terapeutico-assistenziale	Sofisticazione dell'EHR. Il contenuto de dati è lo stesso ma la gestione del PHR è a totale carico del cittadino. Gli ospedali rendono disponibili i dati al cittadino che in ragione al principio di self-determination decide quali dati, come e a chi renderli disponibili. Il cittadino decide come gestire i propri dati dal punto di vista informatico
Coinvolgimento del cittadino	Effettiva Titolarietà dei dati del cittadino ma gestione a carico della struttura organizzativa che li produce	Effettiva Titolarietà dei dati del cittadino ma gestione a carico della struttura organizzativa che li produce	Effettiva Titolarietà dei dati del cittadino ma gestione a carico sia della struttura organizzativa che li produce sia del cittadino	Effettiva Titolarietà dei dati del cittadino e gestione diretta degli stessi da parte del cittadino o di suo delegato (service provider)
Definizione Italiana secondo le Linee guida esistenti	Dossier	Rientra nell'ambito dell' FSE	FSE	Non esiste
Coinvolgimento del cittadino	Titolarietà dei dati del cittadino ma gestione a carico della struttura organizzativa che li produce. In Italia specifico consenso al dossier del cittadino	Titolarietà dei dati del cittadino ma gestione a carico della struttura organizzativa che li produce	Titolarietà dei dati del cittadino ma gestione a carico della struttura organizzativa che li produce. In Italia specifico consenso all'FSE del cittadino che può inserire alcune informazioni	
Dati Trattati	Tutti gli episodi clinici che sono successi nella storia di un cittadino. Ogni episodio può essere composto da più eventi e da più prestazioni erogate in una singola azienda	Tutti gli episodi clinici che sono successi nella storia di un cittadino. Ogni episodio può essere composto da più eventi e da più prestazioni erogate nelle strutture utilizzate dal cittadino	Tutti gli episodi clinici che sono successi nella storia di un cittadino. Ogni episodio può essere composto da più eventi e da più prestazioni erogate nelle strutture utilizzate dal cittadino	Tutti gli episodi clinici che sono successi nella storia di un cittadino. Ogni episodio può essere composto da più eventi e da più prestazioni erogate nelle strutture utilizzate dal cittadino
Tipologia dei processi e dei dati trattati				
area ospedaliera	**episodio di pronto soccorso**: verbale di PS	**episodio di pronto soccorso**: verbale di PS	**verbale PS**	
	episodio ambulatoriale: definizione problema, assessment clinico, referto ambulatoriale	**episodio ambulatoriale**: definizione problema, assessment clinico, referto ambulatoriale	**referto ambulatoriale**	
	episodio di ricovero ospedaliero:assessment clinico e infermieristico, piano diagnostico-terapeutico-assistenziale, diaristica, ciclo del farmaco, prescrizioni SSN, referto sala operatoria, lettera di dimissione, sdo	**episodio di ricovero ospedaliero**:assessment clinico e infermieristico, piano diagnostico-terapeutico-assistenziale, diaristica, ciclo del farmaco, prescrizioni SSN, referto sala operatoria, lettera di dimissione, sdo	**lettera dimissione,** prescrizioni, copia CCE	area CCE ospedaliera
area territoriale	**Esiti esami strumentali**	**Esiti esami strumentali**		
	Esiti imaging	**Esiti imaging**		
	Bilanci di salute	**Bilanci di salute**	Bilanci di salute	
	Igiene pubblica ambientale	**Igiene pubblica ambientale**		
	Igiene pubblica all'individuo	**Igiene pubblica all'individuo**		
	Medicina del lavoro	**Medicina del lavoro**		
	Assistenza consultoriale	**Assistenza consultoriale**		
	Assistenza Domiciliare integrata	**Assistenza Domiciliare integrata**	Adi	
	Piani terapeutici	**Piani terapeutici**	Piani terapeutici	
	Assistenza Residenziale e semiresidenziale	**Assistenza Residenziale e semiresidenziale**	Assistenza Residenziale e semiresidenziale	
	Patient Summary (a cura del MMG)	**Patient Summary** (a cura del MMG)	**Patient Summary**	

Appare inoltre opportuno precisare che l'analisi dei processi organizzativi relativi al percorso diagnostico-terapeutico-assistenziale determina i requisiti organizzativi e informativi del sistema di CCE che andranno tradotti in funzionalità applicative del sistema informatico di CCE.

In tale contesto si ritiene opportuno sottolineare la necessità di una forte sinergia tra revisione dei processi organizzativi e revisione del sistema informativo che deve essere perseguita come requisito di successo del progetto.

Di conseguenza nel seguente documento verranno approfondite tematiche relative ai requisiti organizzativi, funzionali e applicativi della CCE senza particolare enfasi ai requisiti relativi all'infrastruttura tecnologica.



1 —— Definizione CCE ed approccio Aziendale alla CCE

La Cartella Clinica Elettronica (CCE) costituisce un'evoluzione della Cartella Clinica Cartacea (CCC) ovvero è lo strumento per la gestione organica e strutturata dei dati riferiti alla storia clinica di un paziente in regime di ricovero o ambulatoriale, garantendo il supporto dei processi clinici (diagnostico-terapeutici) e assistenziali nei singoli episodi di cura e favorendo la continuità di cura del paziente tra diversi episodi di cura afferenti alla stessa struttura ospedaliera mediante la condivisione e il recupero dei dati clinici in essi registrati.

Le funzioni principali della CCE, riprendendo gli standard di Joint Commission International sono:

- Supportare la pianificazione e la valutazione delle cure (predisposizione del piano diagnostico-terapeutico-assistenziale).
- Costituire l'evidenza documentale dell'appropriatezza delle cure erogate rispetto agli standard.
- Essere lo strumento di comunicazione volto a facilitare l'integrazione operativa tra i professionisti sanitari coinvolti in uno specifico piano diagnostico-terapeutico-assistenziale al fine di garantire continuità assistenziale.
- Costituire una fonte dati per studi scientifici e ricerche cliniche, attività di formazione e aggiornamento degli operatori sanitari, valutazione delle attività assistenziali ed esigenze amministrativo-legali nonché rispondere a esigenze di cost-accounting.
- Supportare la protezione legale degli interessi del paziente, dei medici e dell'azienda sanitaria: deve cioè consentire di tracciare tutte le attività svolte per permettere di risalire (rintracciabilità) ai responsabili, alla cronologia e alle modalità di esecuzione.

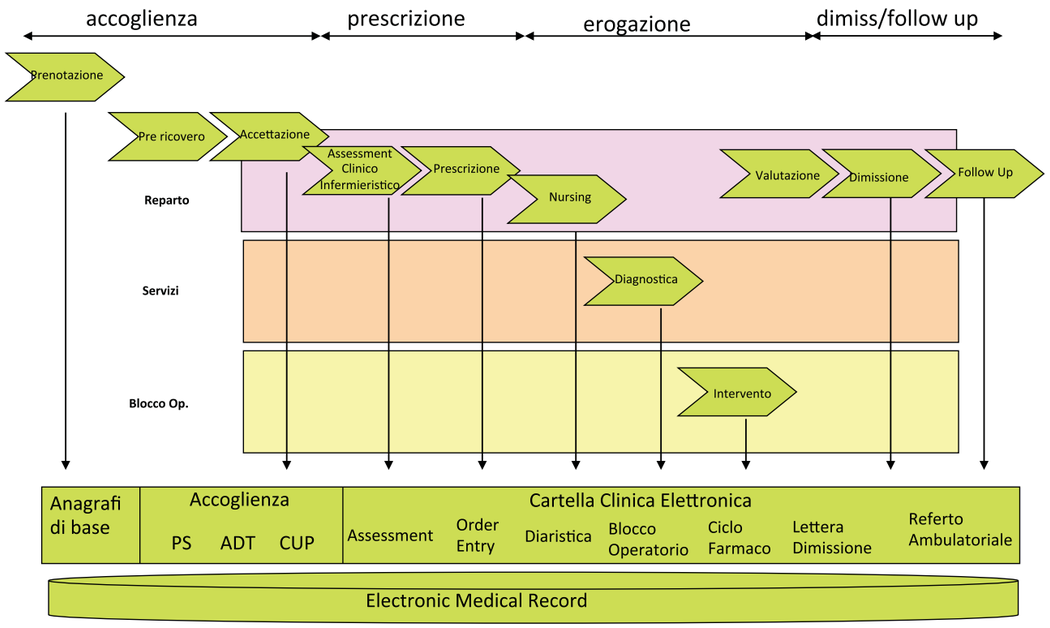
La CCE è pertanto un sistema informatico che contiene tutte le informazioni necessarie per la gestione di un processo diagnostico-terapeutico-assistenziale che di norma comprende informazioni di assessment clinico (anamnesi) e infermieristico (rilevazione dei fabbisogni infermieristici), esame obiettivo, diario clinico integrato (medico e infermieristico), referti di prestazioni ambulatoriali e di altri esami diagnostico-specialistici (ad es. laboratorio, anatomia patologica, radiologia...) gestione del ciclo del farmaco e delle attività di nursing, gestione del percorso chirurgico, gestione della lettera di dimissione con eventuali suggerimenti per il MMG-PLS e di continuità assistenziale, vari documenti amministrativi quali ad es. i consensi informati.
Si ritiene opportuno precisare, riprendendo le indicazioni del documento di Linee Guida della regione Lombardia, che "la CCE si configura quindi come un **sistema informatico integrato aziendale**, da intendersi come trasversale alle varie tipologie di regimi clinico-sanitari di accesso e ai vari processi di cura, in sostituzione della cartella clinica cartacea, che da un lato ne rispetti i requisiti e le funzioni, e dall'altro risolva alcune criticità ad essa legate, offrendo opportunità di aumentare il valore attraverso l'integrazione con altri strumenti informatici. È importante infatti riconoscere allo strumento elettronico una sua dignità che ne determina anche una forte differenza nel modo di assolvere alle sue funzioni rispetto allo strumento cartaceo.
Lo strumento elettronico oggi è in grado di assolvere a tutti i compiti formalmente definiti per la cartella clinica cartacea ma è necessario e auspicabile che lo faccia in modo diverso, ovvero secondo la logica di una efficace ed efficiente gestione elettronica del dato. Per questo motivo, una visione dello strumento di cartella clinica elettronica come il mero "digitalizzatore" del cartaceo, da implementare senza un'adeguata

revisione dei processi interni è riduttiva - se non errata - e non permette di valorizzare il potenziale in termini di gestione integrata delle informazioni, tempestività, automazione, semplificazione offerte dall'ergonomia dello strumento digitale".[1]

1.1 —— CCE come strumento e piattaforma "aziendale" trasversale

Nel paragrafo precedente è stato introdotto il concetto di CCE come strumento e piattaforma "trasversale" aziendale. La CCE intesa come strumento utilizzato per la gestione del processo diagnostico-terapeutico-assistenziale che è suddiviso in fasi che possono essere eseguite in posti diversi, in momenti diversi e da diverso personale clinico-assistenziale è quindi basata su una forte integrazione di processo e, di conseguenza, di tipo informativo. Tra l'altro, parte di questo processo nasce in anticipo sulla fase di ricovero (attraverso attività svolte in regime ambulatoriale e/o di pre-ricovero) e termina formalmente con la dimissione, ma può proseguire con una fase di follow-up ambulatoriale. Appare quindi evidente la necessità che la soluzione informatica garantisca questo livello di integrazione e di trasversalità che è richiesta proprio dal processo organizzativo appena descritto.

La CCE deve quindi intendersi come una piattaforma aziendale trasversale ovvero deve essere utilizzata da tutti i reparti, servizi ambulatoriali e servizi diagnostici per condividere le informazioni necessarie per la gestione dell'intero processo diagnostico-terapeutico-assistenziale sinteticamente illustrato nello schema seguente.



[1] Ripreso da Linee guida per la Cartella Clinica Elettronica Aziendale CRS-LG-SIEE#02, V02.1, 29-02-2012 Regione Lombardia

Appare quindi indispensabile che la CCE sia integrata con la piattaforma aziendale del sistema informativo e che la sua realizzazione dipenda dall'esistenza di alcuni pre-requisiti:

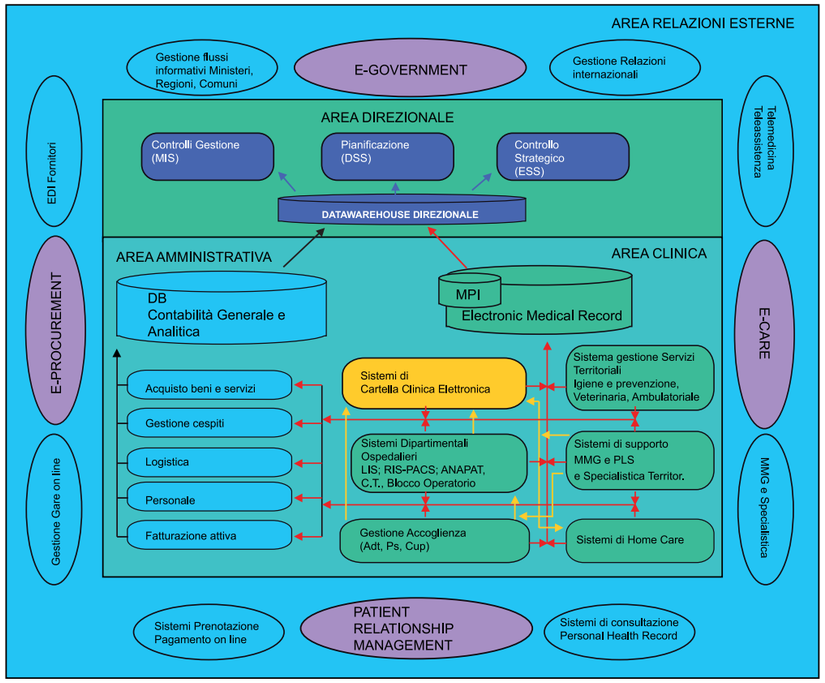
- presenza di un sistema per la gestione di un'unica anagrafe cittadini centralizzata e certificata; ovvero è necessario non solo la presenza informatica di un'anagrafe centrale, ma anche un insieme di regole ben definite e condivise ed una organizzazione aziendale dedicata al suo supporto e mantenimento;
- esistenza di dizionari aziendali condivisi per tutte le "azioni sanitarie" per ottenere uniformità e coerenza di contenuti (terminologie, definizioni, classificazioni, codici) che popoleranno l'insieme delle anagrafi di base del sistema;
- presenza di un sistema centralizzato di programmazione ed accettazione dei pazienti e quindi della disponibilità e integrazione con i sistemi di gestione delle attività di Pronto Soccorso (PS), di gestione delle fasi di Accettazione Dimissione Trasferimento (ADT), di gestione delle prenotazioni ambulatoriali (CUP); presenza di un modulo centralizzato di richieste di prestazioni specialistiche o diagnostiche (CPOE);
  il CPOE "Computerized Physician Order Entry" è un sistema che permette l'inserimento degli ordini verso i servizi diagnostici e ambulatoriali direttamente dalla cartella clinica elettronica e, in modo trasparente per l'utente, inoltrarli al sistema dipartimentale specifico e di riceverne successivamente referti e dati strutturati on line. Tale strumento oltre a rendere più semplice e fluido il flusso di lavoro e la tracciabilità delle attività effettuate ad un paziente, consente di prevenire gli errori e ridurre i tempi di svolgimento del processo;
- presenza di un clinical data repository aziendale che contenga referti e dati strutturati di eventi clinici unitamente con la definizione delle regole di pubblicazione e condivisione dei documenti e metadati;
- definizione dei ruoli degli attori coinvolti che possono essere classificati in tre gruppi: chi fornisce l'assistenza (medici, infermieri, farmacisti, fisioterapisti…), chi utilizza l'assistenza (pazienti), chi gestisce l'assistenza (direttori sanitari, organi istituzionali a livello aziendale e regionale);
- definizione delle politiche di accesso ai dati in termini di profili di autorizzazione all'utilizzo delle varie funzioni di CCE e di regole di privacy da considerare nella gestione dei dati sensibili in essa contenuti. L'importanza della gestione dei profili di autenticazione e autorizzazione sarà trattata specificamente nel 3° capitolo del documento.

1.1.1 Requisiti di interoperabilità

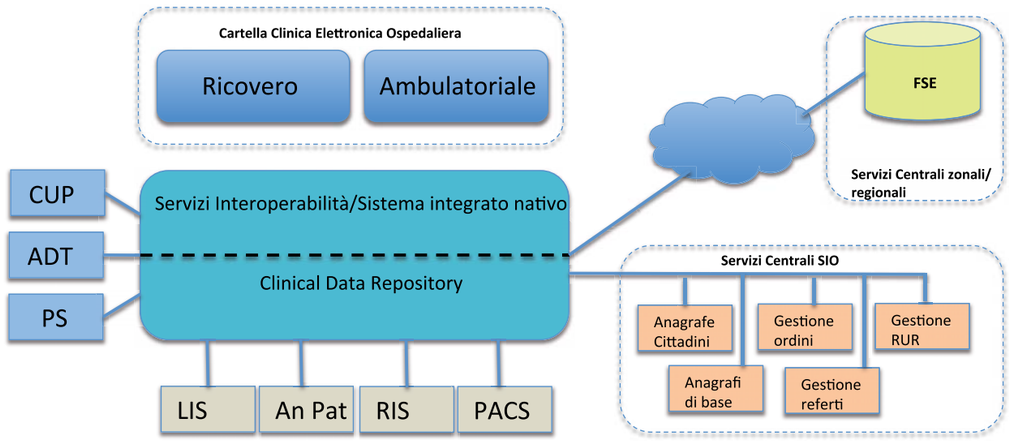
Le considerazioni sopra esposte evidenziano come l'adozione di una CCE all'interno di un'organizzazione sanitaria richieda necessariamente che l'infrastruttura tecnologica consenta un'deguata integrazione tra il sistema di CCE e il sistema informativo aziendale nelle sue componenti cliniche, amministrative e direzionali.

Con riferimento al modello di Health Resource Planning[2], rappresentato nello schema seguente, il sistema di CCE è una delle componenti del Sistema Informativo Ospedaliero che a sua volta può essere una delle componenti del sistema informativo clinico di un'azienda sanitaria. Il sistema informativo dell'area clinica a sua volta deve integrarsi con il sistema informativo dell'area amministrativo-contabile e con il sistema informativo direzionale.

[2] Buccoliero, Caccia, Nasi, e-Health: percorsi di implementazione dei sistemi informativi in sanità, Mc Graw Hill, Milano 2005.



Ancora maggiormente può essere compresa la necessità di un sistema di CCE di tipo trasversale e aziendale che deve garantire integrazione e interoperabilità con tutti i moduli del sistema informativo nel suo complesso e in particolare con quelli che compongono il Sistema Informativo Ospedaliero che verrà approfondito nel capitolo 2 del documento come illustrato nello schema seguente.



Schema del Sistema Informativo Ospedaliero - Aisis

L'interoperabilità tra i vari moduli della CCE può essere garantita sia da un SIO che disponga dei diversi blocchi funzionali già nativamente tra loro integrati, sia da servizi comuni di interoperabilità che garantiscano l'azione coordinata e interoperabile dei differenti blocchi funzionali evidenziati nel paragrafo precedente.

Nell'ambito dell'interoperabilità si richiamano gli standard internazionali Hl7 e Dicom nonchè i profili IHE il cui utilizzo consente di semplificare la condivisione di dati tra moduli applicativi diversi.

A tale scopo nel paragrafo seguente vengono evidenziate le caratteristiche essenziali richieste alla CCE per garantirne un utilizzo omogeneo e coerente, sia quando essa richiede l'interscambio di dati e processi con sistemi organizzativi diversificati (es. quelli indirizzati alle attività amministrative, a quelle diagnostiche, ecc.), sia quando la CCE venga utilizzata in ambiti che richiedono una forte specializzazione clinica.

L'adozione di un'**anagrafica degli assistiti** unica per tutta un'organizzazione sanitaria complessa garantisce la centralità del paziente nel processo di gestione degli episodi clinici all'interno dell'organizzazione stessa.

Analogo ruolo centrale svolge l'**anagrafica delle codifiche** aziendale, che consenta di rappresentare in maniera strutturata gli elementi operativi dell'organizzazione: unità operative, prestazioni offerte, unità erogatrici, centri di costo, profilazione degli operatori, ecc.

I modelli di cura, siano essi specificamente ospedalieri o territoriali, si caratterizzano per processi differenziati per diverse tipologie di episodi clinici, all'interno dei quali le diverse unità operative coinvolte devono poter trattare le informazioni cliniche e amministrative in maniera omogenea, consistente e tempestiva.

Da questo punto di vista, la CCE deve poter essere **integrata con diversi ambiti applicativi** e, a seconda dei contesti, recepire le informazioni che sono già state trattate in fasi precedenti del processo o interagire con fasi successive. Ne sono un esempio gli accessi di **Pronto Soccorso**, per i quali la scheda clinica di PS, alimentata durante il triage e il trattamento in emergenza o gli accertamenti effettuati in **pre-ricovero** che contengono un gran numero di informazioni che devono poter essere acquisite all'interno della CCE, attraverso i meccanismi di comunicazione tra la CCE e i diversi moduli applicativi del SIO.

La CCE deve essere in grado di recepire molti di questi elementi, dalle componenti applicative dedicate all'Accoglienza del paziente con specifico riferimento ai moduli **PS**, **ADT** e **CUP** ma anche di inviare alcune informazioni ad es. procedure chirurgiche, di norma gestite dal modulo chirurgico del sistema di CCE, verso la scheda di dimissione ospedaliera di norma gestita dai sistemi ADT.

Una seconda area critica e particolarmente rilevante di integrazione è costituita dall'attivazione da parte della CCE delle funzioni di gestione richieste (**order entry**) per l'esecuzione di **attività di diagnostica e visite cliniche**. Tale fase, essenziale nel processo diagnostico-terapeutico, deve essere intesa dagli utilizzatori della CCE come una funzione accessibile dall'interno della CCE senza soluzione di continuità rispetto all'operatività sulla CCE. Le richieste devono poter essere formulate dalla CCE con gli stessi criteri e con lo stesso livello di completezza offerti dai moduli applicativi dedicati all'order entry per le unità operative diagnostiche e per le prestazioni specialistiche offerte dai reparti. Analogamente, all'interno della CCE la fruizione diretta di tutti i risultati e i referti prodotti a seguito delle suddette richieste deve agevolare gli operatori utilizzando direttamente o integrando gli strumenti aziendali di consultazione di dati clinici secondo una modalità omogenea nei diversi episodi e esaustiva di tutta la storia clinica di un paziente registrata all'interno della struttura sanitaria.

Il **tracciamento** di un percorso complesso che un paziente in generale può effettuare nelle singole unità operative, inclusivo del dettaglio degli **aspetti clinici** (inquadramenti, diagnosi, referti, ecc.) e degli aspetti **operativi ed amministrativi** (dall'accettazione alla fatturazione delle prestazioni cliniche e dei servizi alberghieri) è un altro elemento essenziale all'interno di un'organizzazione di cura. Ciò richiede che tutti i dati, clinici e amministrativi, strutturati e in forma documentale, siano inseriti in un **Clinical Data Repository Aziendale**

che costituisce, insieme ai servizi di interoperabilità, un pre-requisito di funzionamento. Ciò comporta che la CCE sia in grado di mettere a disposizione dei sistemi esterni le informazioni che possono essere riutilizzate in ambiti diversi.
Considerando le informazioni più significative di un processo di cura, la CCE deve pertanto consentire: l'esposizione dei dati anamnestici acquisiti all'interno di una cartella; la registrazione degli eventi clinici intervenuti nel processo supportato dalla cartella all'interno del sistema informativo aziendale che raccoglie il fascicolo elettronico di un paziente; l'alimentazione con i dati codificati acquisiti nella CCE dei sistemi di rendicontazione aziendale e dei cruscotti direzionali, finalizzati al controllo di gestione e al monitoraggio dei processi aziendali; la costituzione del database clinico disponibile ai fini statistici e di ricerca medica contenente i dati clinici strutturati acquisiti nelle schede (inquadramento medico e infermieristico, epicrisi, ecc.) che compongono la CCE.
Infine, lo sviluppo sempre crescente di scenari in cui il sistema sanitario debba essere inteso in senso ampio, in ambito interaziendale o comunque regionale rende particolarmente importanti gli aspetti di **interoperabilità con i sistemi esterni** all'organizzazione sanitaria, tipicamente costituiti dai Sistemi Sanitari Regionali, da sistemi territoriali pubblici/privati, da reti di patologia o da sistemi per la continuità di cura territoriale con i quali sia necessario interagire attraverso servizi di cooperazione applicativa.
La CCE deve quindi recepire le linee guida e gli standard semantici e tecnologici previsti dai sistemi sanitari regionali e nazionali, in modo che tutte le informazioni e i dati clinici impostati in maniera personalizzata per supportare le esigenze specifiche di un'organizzazione siano riconducibili a quanto previsto dai sistemi esterni con i quali la CCE colloquia.

1.1.2 —— Verticalizzazione/Specializzazione della CCE

I requisiti per la CCE finalizzati a garantire **omogeneità e consistenza** nell'interazione con sistemi aziendali diversificati sono richiesti anche allo scopo di consentire **l'utilizzo di un'unica soluzione di CCE aziendale in modo trasversale alle diverse specializzazioni cliniche**, in grado di supportare l'intero percorso diagnostico-terapeutico-assistenziale trasversalmente ai reparti/servizi in cui si realizzano le varie fasi dello stesso.
In tale contesto un approccio di tipo "specialistico" tende a determinare una forte diversificazione delle modalità di acquisizione delle informazioni cliniche e dei contenuti di una cartella clinica in funzione della disciplina medico-chirurgica di riferimento, e espongono le organizzazioni sanitarie al rischio di adottare soluzioni di CCE diversificate e non integrate .
In proposito si condividono le indicazioni delle Linee guida della Regione Lombardia laddove viene evidenziato che è possibile, pur ribadendo l'importanza di una piattaforma di CCE unica a livello aziendale per garantire la corretta scalabilità clinica della cartella aziendale, che in ambiti operativi ad alta specializzazione possano manifestarsi esigenze di specializzazione degli applicativi, che prevedano una estensione "verticale" della CCE aziendale o una integrazione di moduli applicativi specifici, che aggiungano effettivamente funzionalità rilevanti a quelle già presenti e offerte dalla CCE aziendale. Queste esigenze devono essere attentamente valutate da un lato al fine di salvaguardare il carattere aziendale della CCE (in ottica di continuità di cura), dall'altro lato alla luce degli oneri aggiuntivi economici e di gestione derivanti dalla necessità di mantenere

allineati ed operativi più prodotti di "nicchia". È opportuno, in ragione a tali considerazioni, motivare adeguatamente la necessità e l'esigenza di mantenere operativi eventuali applicativi verticali. Per tali applicativi è richiesto che vengano garantiti i requisiti minimi di sicurezza, interoperabilità, integrazione al SIO, normativi e di business continuity che sono prescrittivi per la soluzione di CCE aziendale e che devono essere mutuati anche dai prodotti di specialità (verticali), proprio in ottica di massima affidabilità e integrazione nella gestione dei dati clinici del paziente.
In tale contesto appare importante evidenziare una serie di moduli con forte caratterizzazione "aziendale" (referto ambulatoriale, verbale operatorio, lettera di dimissione, area infermieristica, ciclo del farmaco, diaristica) e una serie di moduli (inquadramento clinico ed esame obiettivo) che possono adattarsi alla disciplina nella quale viene utilizzata.
Ciò comporta che la CCE possa quindi includere tra le proprie funzioni integrate un ambiente di amministrazione specificamente dedicato alla parametrizzazione/personalizzazione dei contenuti delle sezioni che compongono una cartella clinica. Tali elementi di personalizzazione vanno dalla possibilità di adattare alle specifiche esigenze di una disciplina medica i modelli elettronici che consentono di compilare le sezioni della CCE sopraindicate, alla possibilità di utilizzare una presentazione grafica arricchita per agevolare gli operatori medici e infermieristici.
Per coordinare uno sviluppo organico e definire una base comune di informazioni è indispensabile un supporto organizzativo e sanitario. È pertanto fondamentale definire un gruppo di lavoro multidisciplinare, a livello aziendale, che definisca le linee guida comuni per la CCE aziendale, come successivamente approfondito nel capitolo 4.

1.2 —— CCE come fattore abilitante per FSE e PHR

Negli ultimi anni in ambito sanitario è cambiato il concetto di valore del servizio. Il primo cambiamento è stato un diverso approccio al modello di erogazione del servizio: il focus non è più sulla malattia o sulla singola prestazione ma è sul paziente. Questo cambia radicalmente la progettazione dei sistemi informativi e dei sistemi informatici passando da progetti "aziendali" e "limitati" a progetti interaziendali. In uno scenario di questo tipo, "paziente-centrico", l'introduzione di sistemi informativi integrati ed evoluti è fondamentale per la gestione del paziente e delle informazioni cliniche che lo riguardano, al fine che esse possano essere condivise e messe a disposizione dei diversi professionisti che entrano a far parte del processo diagnostico-terapeutico-assistenziale del paziente.
Come indicato nell'introduzione del documento, esistono diversi modelli di sistemi informativi. Di seguito vengono riportate le definizioni di alcuni di essi, prendendo a riferimento la classificazione del Medical Record Institute (MRI). L'EMR (Electronic Medical Record) è un'architettura orientata alla gestione integrata dei flussi informativi dell'area clinico-sanitaria di un'azienda con l'obiettivo di assicurare un governo complessivo del percorso diagnostico-terapeutico-assistenziale (Caccia, 2008). Nella legislazione italiana l'EMR è paragonabile al "DOSSIER" di cui alle linee guida sul FSE del Garante della Privacy e del Ministero della Salute. Esso consente la gestione di tutti i contatti di un cittadino con qualsiasi servizio dell'azienda sanitaria (o di un'azienda con unico titolare del trattamento). In tale contesto la CCE è un subset informativo dell'EMR o del dossier.

Le architetture EPR (Electronic Patient Record) ed EHR (Electronic Health Record) sono architetture basate su sistemi EMR ma hanno un ambito di operatività più ampio, ovvero sono soluzioni condivise da professionisti che operano in strutture diverse distribuite sul territorio. L'EHR è similare al Fascicolo Sanitario Elettronico che, facendo riferimento al documento del Ministero della Salute "Il Fascicolo Sanitario Elettronico Linee guida nazionali" del 2010, viene definito come: "l'insieme dei dati e dei documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito. Il Fascicolo Sanitario Elettronico, che ha un orizzonte temporale che copre l'intera vita del paziente, è alimentato in maniera continuativa dai soggetti che prendono in cura l'assistito nell'ambito del Servizio Sanitario Nazionale e dei servizi socio-sanitari regionali".

Un altro importante cambiamento emerso degli ultimi anni in sanità è la necessità di migliorare l'interazione con i cittadini, consentendo agli stessi di poter accedere e gestire direttamente i propri dati clinici. Il sistema PHR (Personal Health Record), diffuso soprattutto nel contesto nord-americano, consiste in un approccio ai dati clinici che prevede la messa a disposizione dei dati clinici, prodotti dai sistemi EMR/EHR, direttamente al cittadino che può gestirli autonomamente o tramite un provider da lui scelto. Caratteristica di tali sistemi è la gestione, dei dati e delle informazioni effettuata dal paziente stesso il quale, in quanto proprietario del dato, decide a chi e quando consentirne l'accesso, con una considerevole riduzione delle criticità legate alla complessità delle infrastrutture di EHR e alle problematiche legate alla privacy.

Dalle considerazioni sinteticamente evidenziate risulta pertanto evidente che architetture quali la CCE e l'EMR costituiscono uno dei pre-requisiti per la costituzione di architetture EHR (FSE) o PHR. L'assenza di tali pre-requisiti rende difficilmente sostenibile la realizzazione di queste architetture di condivisione di dati clinici.

1.3 ——— CCE e modello assistenziale per intensità di cura

L'Ospedale per intensità di cura è un modello organizzativo che tende a caratterizzare l'ospedale, in continuità con un "lungo" processo di cambiamento, come un luogo di cura delle patologie acute.

Questa nuova connotazione, richiede sia una revisione organizzativa dei processi ospedalieri sia una riqualificazione dell'offerta territoriale tale da garantire la continuità terapeutico-assistenziale dalla cui efficienza dipende l'appropriatezza del ricovero ospedaliero e un'efficace gestione della dimissione precoce.

Un fattore abilitante nella realizzazione di una maggiore integrazione tra diverse figure professionali, che garantisca una risposta globale ed esauriente ai bisogni del paziente gestito sia a livello territoriale sia a livello ospedaliero, è la condivisione delle conoscenze sul paziente da parte dei professionisti che sono coinvolti nella gestione di un dato paziente e l'implementazione di strumenti di comunicazione che rendano più snelli i passaggi tra ospedale e territorio e in generale nelle varie fasi del processo diagnostico-terapeutico-assistenziale ospedaliero.

L'integrazione dei percorsi clinici rappresenta lo strumento fondamentale perché possa essere realizzata la nuova presa in carico che vede la centralità del paziente come filo conduttore della riorganizzazione dell'ospedale per intensità di cura tramite l'integrazione delle competenze professionali e l'uniformità dei processi di cura orientati alle migliori evidenze cliniche. Questo nuovo asset organizzativo sposta quindi l'attenzione dai processi di lavoro (Radiologia, Laboratorio di analisi, …) ai percorsi clinici del paziente.

Il modello per intensità di cura viene normalmente strutturato in 3 livelli:

- il livello 1 unificato comprende la terapia intensiva e subintensiva;
- il livello 2, articolato almeno per area funzionale, comprende il ricovero ordinario e il ricovero a ciclo breve che presuppone la permanenza di almeno una notte in ospedale (week surgery, one-day surgery);
- Il livello 3 unificato è invece dedicato alla cura delle post-acuzie o low care.

I "percorsi" implementati dagli attuali sistemi di accettazione ospedaliera che prevedono l'associazione univoca paziente-reparto non sono più sufficienti a supportare il nuovo modello per intensità di cura.

Per poter gestire questo nuovo modello, ma anche la transizione verso questa nuova organizzazione attraverso una soluzione ibrida, è necessario introdurre nuovi concetti all'interno dei sistemi ADT e CCE.

Nel sistema ADT il paziente deve essere associato a due diverse tipologie di "entità":

- L'Unità Operativa di Ricovero (che individua la competenza medica)
- L'Unità di Degenza (che individua la competenza assistenziale infermieristica)

Le situazioni in cui un paziente, nel corso del proprio percorso ospedaliero, debba essere preso in carico da un'equipe infermieristica diversa da quella dell'Unità Operativa di Ricovero, la cui equipe medica mantiene invece la competenza clinica sul paziente, possono essere gestite mediante il concetto di Unità di Degenza.

La distinzione tra Unità di Degenza e Unità Operativa di Ricovero deve essere mantenuta nelle fasi di accettazione, trasferimento e nelle operazioni di ricerca.

Si rende dunque evidente la necessità di disporre uno strumento che permetta una visione trasversale che renda possibili tutte le fasi del percorso. In particolare dal momento in cui viene effetuata la valutazione iniziale dell'intensità di cura fino alle successive rivalutazioni di questo percorso in conseguenza del mutare delle condizioni del paziente.

La Cartella Clinica integrata in questo nuovo modello diviene quindi il principale strumento di integrazione professionale, comune tra le varie figure professionali che intervengono sul paziente.

Questo strumento, che dovrà accompagnare il paziente in tutte le fasi dell'intensità di cura, rappresenta uno dei presupposti della continuità e della personalizzazione dell'assistenza.

Tale strumento deve essere costruito in modo da essere fruibile da tutti gli operatori coinvolti nel processo assistenziale, e deve fornire l'informazione che serve, dove serve, nel modo adeguato ed esclusivamente a chi è deputato a farne uso.

1.4 ——— CCE e continuità terapeutica-assistenziale ospedale-territorio

La realizzazione dei percorsi integrati di continuità di cura ospedale - territorio finalizzati alla presa in carico del paziente dall'inizio dell'esordio fino al completamento del suo percorso di cura richiedono una forte integrazione tra le attività effettuate in regime di ricovero e la programmazione e gestione del paziente dopo la dimissione. Tale integrazione è particolarmente rilevante per pazienti di tipo cronico e/o in condizioni di non autosufficienza.

L'utilizzo di una CCE che contenga tutte le informazioni anagrafiche e socio-sanitarie utili, nonché tutte le informazioni necessarie per il trattamento del paziente in ospedali a bassa intensità o in assistenza domiciliare, sta diventando un elemento sempre più importante. Le informazioni devono essere inserite già in fase di

accettazione e nei primi giorni di ricovero in modo da permettere di informare tempestivamente la struttura territoriale.

Appare quindi necessario prevedere una integrazione tra la CCE attiva presso le strutture ospedaliere e gli applicativi informatici utilizzati a livello territoriale per l'assistenza della residenzialità, l'assistenza domiciliare integrata e con i sistemi utilizzati da MMG e PLS.

Tale integrazione può essere realizzata con diverse modalità: dalla condivisione di database, alle realizzazione di "servizi" che consentano uno scambio di dati mediante utilizzo di standard semantici, alla realizzazione di Patient Summary.

In questo documento si vuole solo richiamare l'attenzione sulla necessità che in fase di progettazione dei sistemi di CCE ospedaliera si tenga conto anche di questo importante livello di integrazione che può costituire un utile supporto ai processi di continuità di cura.

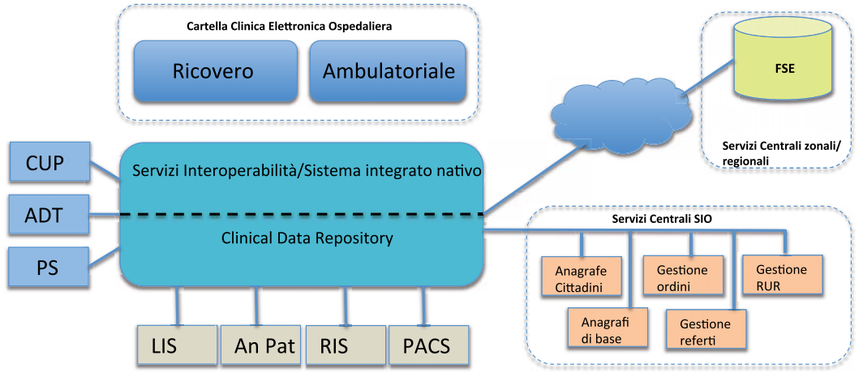
2 —— Funzionalità della CCE

Nella realizzazione di un sistema di CCE, come già accennato nella parte introduttiva del presente documento, devono essere considerati aspetti organizzativi, funzionali e applicativi affinchè la CCE possa essere uno strumento informatico di valido supporto agli operatori sanitari nella gestione del processo diagnostico-terapeutico-assistenziale all'interno di una struttura ospedaliera.

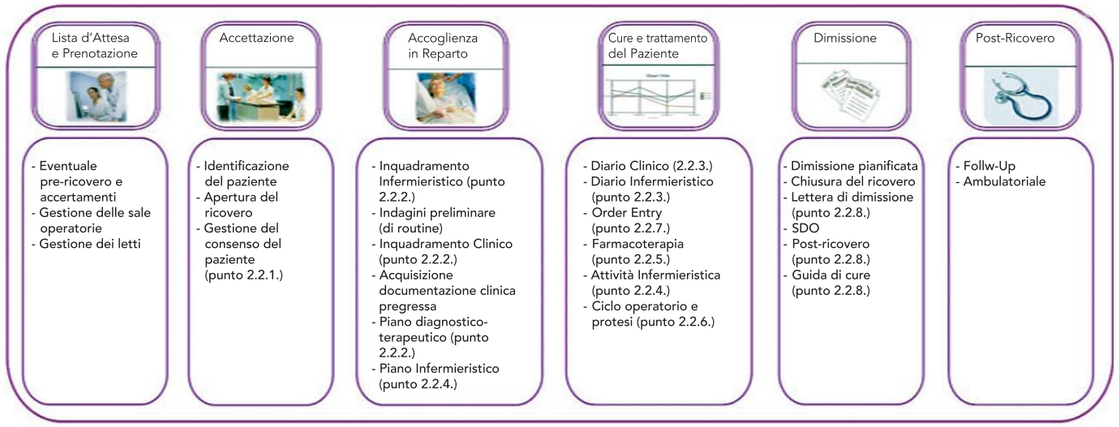
In questo capitolo verranno elencati i requisiti minimi obbligatori che uno strumento di CCE deve possedere dal punto di vista funzionale/applicativo.

Verranno inoltre fatte alcune brevi considerazioni di carattere tecnologico sulle possibili soluzioni applicative senza l'obiettivo di essere esaustivi nel trattare la materia ma, semplicemente, per richiamare l'attenzione su alcuni aspetti di valutazione che si ritengono significativi.

Appare opportuno, in tale contesto, riprendere lo schema del SIO per focalizzare di nuovo lo scenario di riferimento di un sistema di CCE ed il fatto che la sua realizzazione non può prescindere dall'esistenza delle altre componenti del SIO, che ne costituiscono un pre-requisito, e dall'integrazione con le stesse.



Di seguito si riporta lo schema di processo semplificato che sintetizza le principali fasi dello scenario relativo al ricovero ordinario e, per ciascuna fase, si elencano le principali attività che possono essere svolte e quindi le funzionalità di supporto che gli strumenti informatici devono implementare. In appendice del documento vengono illustrati altri esempi di schemi di processo, che mostrano come si potrebbe procedere in un'attività di analisi dei processi ospedalieri, propedeutico alla definizione di una fase progettuale di "to be".



È importante chiarire che la CCE è un supporto informatico per la gestione di dati e processi nel percorso di cura di un paziente: non si tratta pertanto di una semplice collezione di documenti che, nei fatti, sono solo uno dei prodotti della gestione stessa del processo. Il sistema di CCE deve essere quindi orientato al processo medico/infermieristico che ovviamente prevede la generazione e la consultazione di dati e documenti ma non si limita solo a questo aspetto.
Nel processo di implementazione della CCE infatti è necessario tenere in considerazione che molte delle consuetudini nella gestione della CCC sono state profondamente determinate dallo strumento cartaceo utilizzato.
Il nuovo contesto informatico può e deve consentire di introdurre importanti migliorie nella gestione e nell'organizzazione dei dati rispettandone i requisiti di completezza e di integrità. Appare quindi opportuno evitare di riproporre pedissequamente, con il nuovo strumento, le stesse modalità di lavoro necessarie al supporto cartaceo e cogliere invece le opportunità offerte dalle tecnologie informatiche in termini di fruibilità, semplificazione, integrazione e condivisione delle informazioni.

2.1 —— Elementi tecnologici della CCE

Come detto più sopra si ritiene opportuno richiamare l'attenzione su alcuni aspetti tecnologici che caratterizzano i sistemi di CCE e che ne condizionano l'attivazione e l'uso, con particolare riferimento all'interfaccia grafica utente, alle sue tecnologie di sviluppo e ai dispositivi di utilizzo.

2.1.1 —— Tecnologie software di sviluppo

La tecnologia utilizzata per lo sviluppo di un sistema di CCE, ma anche di qualsiasi sistema informativo, ne condiziona l'efficienza, l'usabilità e anche la manutenibilità. A tale scopo, nella tabella seguente si elencano diverse tecnologie utilizzabili nello sviluppo applicativo evidenziandone criticità e vantaggi.

Front End	Vantaggi	Criticità
Client/Server	*Funzionalità ricche*	*Troppo legato al Sistema Operativo, difficoltà di aggiornamento, difficoltà di manutenzione*
VDI	*Funzionalità ricche, facilità di gestione e manutenzione, follow me desktop*	*Necessità di accurata valutazione dei costi di switch-off*
Web (HTML5)	*Maggior portabilità determinata dal solo utilizzo di un browser*	*Interfaccia utente meno ricca, impossibile in alcuni casi fare caching locale di dati o altro (per scopi di performance e Business Continuity), difficoltà a sfruttare le periferiche locali del device (es. lettore di smartcard)*
Web (RIA, ad es. Java, Adobe AIR, ...)	*Funzionalità ricche*	*Legato ad installazioni o componenti sw locali, difficoltà di aggiornamento*
App locale (per tablet e smartphone)	*Funzionalità ricche e pieno sfruttamento del mondo tablet (pinch, zoom, ecc).*	*Legato al device, costi di aggiornamento*

Allo stato dell'arte si suggerisce di valutare adeguatamente i dispositivi che si intendono adottare per l'utilizzo della CCE in quanto tale scelta è fortemente vincolata alla tipologia di tecnologia d'implementazione della soluzione. È probabile che le realizzazioni di sistemi complessi di CCE richiedano soluzioni "miste".

2.1.2 —— Interfaccia

Il processo gestito dalla CCE è articolato e complesso, ciò nonostante l'interfaccia utente della CCE deve essere intuitiva e guidare l'utente finale attraverso un percorso logico rispettoso, nelle sequenze e nella nomenclatura, del processo medico ed infermieristico.
La CCE dovrà essere orientata sia alla "vista d'insieme" sia all'evidenza di eventuali allarmi in merito a quanto sta accadendo.
La CCE deve avere un'interfaccia utente che sia al tempo stesso semplice, accattivante, facile da capire e da usare. Idealmente l'interfaccia dovrebbe essere la stessa per tutte le funzioni della CCE e per i diversi tipi di dispositivo. Preso atto dell'estrema variabilità dei dispositivi utilizzati appare quantomeno necessario che l'interfaccia sia molto simile nell'aspetto e nei modi d'uso, così da ridurre al minimo i tempi di apprendimento e di adattamento.
Si suggerisce inoltre che la CCE non induca l'operatore a non ragionati "copia-incolla" come indicato da JCI.
Anche la fruibilità dei dati deve essere orientata all'utente, privilegiando il più possibile i paradigmi grafici (disegni, linee temporali, reparto come insieme di letti, processo medico-infermieristico come sequenza di attività, ecc.), rispetto a griglie o a semplici elenchi (che possono comunque essere presenti, perchè utili ad utenti più evoluti o, ad esempio, in situazioni in cui è necessario rinunciare alla grafica).
Come già evidenziato, l'implementazione di un sistema di CCE si sviluppa al di sopra di un datarepository clinico il cui paradigma informatico tipicamente è quello di un contenitore i cui elementi si inseriscono in una struttura gerarchica ad "albero". La CCE deve garantire la navigabilità di questi dati secondo la loro gerarchia ma, auspicabilmente, deve consentire che i diversi "oggetti" o "eventi" che compongono la cartella, siano essi richieste, documenti, valori numerici e così via, siano anche rintracciabili, ricercabili e raggruppabili mediante altri criteri, che rendano possibili anche viste "trasversali" alla struttura principale dell'albero.
Ad esempio si può pensare a criteri di raggruppamento delle informazioni cliniche che mostrino tutti gli eventi legati alla cardiologia, oppure tutti i valori ematici fuori soglia, o tutte le TAC, o tutti i referti chiesti con un certo quesito diagnostico e così via. Ovviamente tra queste viste trasversali sarebbe auspicabile poter disporre della dimensione temporale nelle possibili interrogazioni. Gli stessi criteri di raggruppamento dovrebbero essere disponibili sia a livello di Dossier sia a livello di fascicolo sanitario.
I dati prodotti durante la gestione del paziente sono la base per eventuali successive analisi cliniche, epidemiologiche e gestionali sviluppate mediante l'utilizzo di tecnologie di "Business Intelligence".

2.1.3 ——— Dispositivi di accesso alla CCE

Esistono diversi dispositivi che consentono l'utilizzo della CCE. Nello schema seguente vengono evidenziati

criticità e vantaggi dei vari dispositivi. È opportuno che il criterio principale di scelta sia legato ai casi d'uso (scenari di utilizzo) a cui il dispositivo è destinato: in corsia o in sala infermieri, usato dal medico o dall'infermiere, durante il giro visite o per le attività infermieristiche al letto del paziente, e così via.
Anche in questo caso, vista l'estrema variabilità degli atti clinico-sanitari si può ipotizzare l'utilizzo di dispositivi diversi a seconda della funzionalità e/o del caso d'uso.

Device	Vantaggi	Criticità
Smartphone	*Dimensioni, peso, particolarmente adatto ad alcune funzioni (es. parametri vitali)*	*Dimensioni limitate dello schermo. Limiti nell'accesso ad alcune funzioni della CCE. Necessita di accurata valutazione della configurazione wifi. Autonomia elettrica*
Tablet	*Interessante rapporto tra portabilità e disponibilità del contenuto informativo*	*Non consente l'uso a mani libere, poco adatto a data entry di tipo descrittivo, rischio di furto. Autonomia elettrica*
Carrello informatico o pc portatile su carrello	*Risoluzione e grandezza schermo ottimali; buon rapporto tra portabilità e disponibilità del contenuto informativo, collegabile alla rete fissa in caso di emergenza sulla parte wireless*	*Soluzione ingombrante, necessita di valutazione sull'ergonomia del carrello. Autonomia elettrica*
PC al letto	*Risoluzione e grandezza schermo ottimali; ottimo rapporto tra portabilità e disponibilità del contenuto informativo, consente il massimo delle funzionalità di gestione e visualizzazione dei dati clinici e delle immagini al letto del paziente. No problemi di autonomia elettrica*	*Costo della soluzione*

2.2 ——— Funzionalità minime della CCE

In questo capitolo vengono elencate le funzionalità applicative minime richieste per la realizzazione di un sistema di CCE.

2.2.1 ——— Acquisizione consensi del cittadino e documentazione "terza"

All'ingresso in reparto, se il consenso al trattamento non è stato acquisito in fase di accettazione amministrativa, è necessario acquisirlo. Appare evidente che se il consenso è già stato acquisto, tale informazione deve essere trasmessa dal sistema di ADT alla CCE. In proposito si evidenzia che l'acquisizione del consenso direttamente in forma digitale richiede l'attivazione di procedure e strumenti che sanciscano l'integrità del documento di rilascio del consenso. In caso contrario se il consenso viene acquisito in forma cartacea nella CCE deve quantomeno essere riscontrabile "la sua avvenuta acquisizione". Queste considerazioni si applicano a tutte le firme di consenso che il cittadino dovrà rilasciare durante il percorso diagnostico-terapeutico-assistenziale. È possibile che nella fase di accoglienza il cittadino fornisca documentazione (anche di carattere multimediale) relativa a eventi o episodi clinici precedenti. In tal caso è opportuno che il sistema di CCE consenta l'acquisizione di tale documentazione che, non essendo "certificata" dovrà costituire degli allegati della CCE.
Il sistema di CCE deve consentire l'acquisizione automatica delle informazioni inserite e degli esami richiesti in regime di pre ricovero, se effettuati nella stessa struttura. Medesima considerazione vale per le informazioni cliniche derivanti da prestazioni post ricovero qualora la normativa preveda che le stesse siano ricomprese nel ricovero.
Per completezza si evidenzia che alcune regioni stanno avviando tavoli tecnici al fine di consentire una standardizzazione dei formati di interscambio dei dati clinici. In questo caso sarà oggettivamente possibile importare nel sistema CCE dati esportati da sistemi CCE di altre strutture sanitarie.

Funzionalità obbligatorie	Note/Dettaglio
*Acquisizione del **Consenso al trattamento dati.*** *Autorizzazione del paziente al trattamento dei dati (Codice della privacy e correlati provvedimenti del Garante per la protezione dei dati personali).* *Il consenso al trattamento dei dati deve per esempio essere espresso dal paziente nei seguenti casi:* *- affinché l'Azienda Ospedaliera possa creare un Dossier Clinico a livello aziendale* *- affinché l'Azienda Ospedaliera possa memorizzare i dati clinici del paziente in un FSE per esempio a livello regionale se presente* *- prima della partecipazione del paziente a protocolli di ricerca, indagini e sperimentazioni cliniche.*	*Selezione del tipo di consenso/template predefinito e stampa del foglio informativo da far firmare al paziente.*
*Acquisizione del **Consenso informato**.* *Il consenso informato è acquisito in diverse occasioni lungo il processo clinico: interventi chirurgici, anestesia, utilizzo di sangue od emocomponenti ed altri trattamenti e procedure ad alto rischio (escluse emergenze). Lo stesso modulo consente poi la raccolta del consenso specifico per gli interventi specialistici in regime ambulatoriale (es. interventi odontoiatrici, interventi dermatologici) secondo il template definito a livello aziendale.* *In generale in tutti i casi di intervento specialistico invasivo o a rischio, trattamento terapeutico, partecipazione a sperimentazioni cliniche.*	*Selezione del tipo di consenso/template predefinito e stampa del foglio informativo da far firmare al paziente.*

Funzionalità obbligatorie	Note/Dettaglio
*Acquisizione **documentazione cartacea di terze parti**.*	*Acquisizione da file system (e/o scanner).*
***Consultazione** della storia clinica precedente del paziente.* *I contenuti del repository clinico aziendale di potenziale interesse sono:* *- Relazioni ambulatoriali, referti ambulatoriali* *- Referti di diagnostica o visite-parere* *- Lettera di dimissione* *- Verbali operatori* *- Verbali di pronto soccorso*	*Trasversalmente all'episodio in corso, a prescindere dal regime di accesso del caso, il sistema deve permettere:* *- la condivisione di dati in forma strutturata delle fasi precedenti e successive del percorso di cura del paziente e l'importazione di contenuto presente nei referti precedenti dello stesso ambulatorio (referto ambulatoriale) o reparto (lettera di dimissione) nei rispettivi campi tematici (richiedendo una esplicita conferma degli stessi al clinico).* *- la consultazione dei documenti deve essere possibile sia in forma strutturata, sia in forma di referto pdf.*
Recupero e condivisione dati clinici. ***Importazione** dati clinici precedenti (da pre ricovero, da precedente ricovero o visita ambulatoriale) per esempio in fase di compilazione di una lettera di dimissione o di un referto ambulatoriale.*	*Deve essere possibile la condivisione di dati in forma strutturata con le fasi precedenti e successive del percorso di cura del paziente. Ad esempio, la sintesi anamnestica di una visita ambulatoriale di pre ricovero o le terapie in corso potrebbero andare a popolare l'anamnesi che il medico di reparto compilerà in fase di ricovero.* *Analogamente, i dati di ricovero potrebbero alimentare la refertazione di una visita ambulatoriale di follow-up, ed il sistema di CCE deve essere predisposto per un loro recepimento da ogni genere di referto prodotto dal sistema di CCE aziendale o da soluzioni verticali dell'Ente.*

2.2.2 —— Assessment medico e infermieristico

Il paziente, arrivato in reparto, viene preso in carico dal team medico-infermieristico attraverso l'attività di inquadramento clinico ed infermieristico.

L'obiettivo dell'inquadramento clinico è quello di predisporre, in base al problema emergente per il quale il paziente è stato ricoverato, il piano diagnostico-terapeutico.

L'assessment infermieristico è la fase del processo di cura in cui l'infermiere effettua una valutazione dei fabbisogni infermieristici del paziente indipendentemente dal motivo di ricovero per definire il piano assistenziale.

Di solito, viene utilizzato un quadro di valutazione, basato su modelli di assistenza italiani o internazionali che la CCE deve recepire.

L'insieme delle due valutazione determina il piano diagnostico-terapeutico-assistenziale che, nei fatti, guiderà tutte le attività erogate al paziente.

Si segnala in proposito che, secondo le indicazioni di JCI, le attività di assessment dovrebbero essere completate entro le prime 24 ore dall'ingresso in reparto.

Funzionalità obbligatorie	Note/Dettaglio
***Inquadramento clinico iniziale/all'ingresso**.* *Da eseguire di norma entro le 24 ore dall'accettazione e comunque prima di anestesia o di trattamento chirurgico, ovvero secondo specifiche regole aziendali definite. Spesso tali valutazioni, anche se condotte nella fase di pre ricovero (ad esempio tipicamente nei casi di chirurgia d'elezione) sono comunque da considerarsi parti integranti il ricovero e quindi della Cartella Clinica Elettronica.*	*- Motivo del ricovero* *- Anamnesi (familiare, fisiologica, patologica remota, patologica prossima)* *- Reazioni avverse, intolleranze, allergie (ambientali, alimentari, farmacologiche)* *- Terapie pregresse ed in atto (devono essere raccolte, registrando indicazioni circa i farmaci in uso e la relativa posologia, con esplicitazione dei farmaci che il paziente ha portato con sé dal domicilio)* *- Elenco dei problemi del paziente* *- Esame Obiettivo* *- Ipotesi diagnostiche* *- Piano diagnostico-terapeutico previsto, descrizione dei fabbisogni e finalità assistenziali, compresi i parametri vitali da monitorare.*
***Valutazione infermieristica all'ingresso**.* *L'elaborazione di una cartella infermieristica richiede, quale presupposto, l'adozione di un modello concettuale di riferimento (ad esempio la teoria dei bisogni).*	*Devono essere valutate le condizioni del paziente che necessitano di attività assistenziali: a seconda del modello di accertamento scelto devono essere rilevati i bisogni assistenziali o valutate le condizioni del paziente relativamente alle diverse aree funzionali e fissati gli obiettivi dell'assistenza.* *Tipicamente vengono compilate una o più schede di valutazione delle condizioni del paziente, per registrare gli aspetti di cui sopra, evidenziando ad esempio:* *le manifestazioni (aspetti oggettivi e soggettivi)* *gli obiettivi da raggiungere con l'assistenza.* *Ad esempio, devono poter essere rilevati e valutati i seguenti aspetti:* *- Informazioni relative ad ausili e presidi in dotazione a domicilio* *- Valutazione di vista, udito e capacità comunicative* *- Valutazione dei bisogni assistenziali del paziente quali ad esempio quelli relativi alle necessità di respirazione, alimentazione e idratazione, eliminazione urinaria e intestinale, igiene, movimento, riposo e sonno, funzioni cardiocircolatorie, ambiente sicuro, interazione nella comunicazione, procedure terapeutiche, procedure diagnostiche* *- Necessità di attività pre-operatorie: preparazione del paziente ad un intervento chirurgico* *- Necessità di attività post-operatorie: attività sul paziente al rientro in reparto dopo l'intervento chirurgico.* *Sulla base delle informazioni così raccolte vengono poi definite le attività assistenziali (compresa la rilevazione dei parametri vitali) da effettuare sul paziente che devono essere pianificate secondo un piano assistenziale. Il piano assistenziale viene periodicamente aggiornato a fronte di rivalutazioni del paziente effettuate nel corso della degenza.*

Funzionalità obbligatorie	Note/Dettaglio
Scale di valutazione	*Le scale di valutazione possono essere compilate da personale sia medico sia infermieristico.* *Esempi comuni di scale sono:* *- Valutazione del dolore* *- Autonomia paziente* *- Rischi di caduta* *- Rischio/valutazioni di lesioni da decubito* *- Rischio di malnutrizione*

2.2.3 ——— Diaristica

La diaristica medica, infermieristica e riabilitativa raccoglie i dati relativi all'evoluzione del paziente e la sua risposta al trattamento. Tali dati vengono raccolti periodicamente, se necessario anche più volte al giorno.
In ogni annotazione devono figurare nome e cognome dell'operatore e data e ora dell'effettuazione dell'attività. La certezza del tracking informativo viene ulteriormente approfondita nel capitolo 3.
In automatico il sistema potrebbe generare delle registrazioni nel diario a seguito di "eventi" come le richieste di esami, le rilevazioni dei parametri vitali…; alternativamente potrebbe essere sufficiente la possibilità di visualizzare o importare questi dati a richiesta.
Nel diario infermieristico, oltre alle informazioni sull'evoluzione del paziente, viene raccolto un riassunto delle attività realizzate dal personale infermieristico. I dati raccolti nel diario aiutano a documentare la frequenza e l'estensione delle varie attività clinico-assistenziali e la reazione del paziente al trattamento.

Funzionalità obbligatorie	Note/Dettaglio
Nella loro forma base, le annotazioni possono essere costituite da semplici inserimenti in forma di un unico campo di testo libero organizzate cronologicamente all'interno di un elenco di giornate di degenza.	*I diari possono essere gestiti separatamente, ad esempio uno per ogni figura professionale o profilo specifico (es. farmacista, fisioterapista), oppure convergere in un unico diario condiviso tra più ruoli, ad esempio sulla base del modello del diario clinico – assistenziale, leggibili e filtrabili sia cronologicamente che per profilo professionale, con possibilità di "switch" tra la vista dei singoli diari e una vista trasversale (l'integrazione dei diari è ritenuta utile per facilitare il coordinamento e l'allineamento del personale di reparto nell'assistenza e cura del paziente).* *In quest'ultimo caso è necessario che la profilazione degli utenti garantisca l'aderenza alle policy aziendali di accesso ai dati in lettura e scrittura e che ciascun inserimento sia profilato sul ruolo dell'autore (ad esempio personale medico ed infermieristico).* *Nel caso del diario infermieristico si potrebbe strutturare il diario in categorie, che rappresentino funzioni valutate del paziente (es. categoria nutrizionale, in modo da facilitare il seguimento e controllo di determinate funzioni chiave per la salute del paziente.)*

Funzionalità obbligatorie	Note/Dettaglio
Possibilità di mettere in evidenza specifici inserimenti o parti di essi rispetto al circostante testo, al fine di renderli maggiormente visibili all'utente attraverso ausili grafici (es. formattazione, colori, simboli).	*Opzionalmente anche la possibilità di agganciare dati strutturati o dati multimediali (foto, video, voce).*

2.2.4 ——— Attività di nursing

Si definisce così il processo che porta a pianificare le attività infermieristiche sul paziente e le rilevazioni dei suoi parametri vitali e che scaturisce da un'analisi dei singoli bisogni del paziente, che avviene attraverso un'opportuna raccolta di informazioni specifiche per ciascun bisogno.
Da questa analisi il personale infermieristico è in grado d'impostare un obiettivo legato al bisogno e la data del suo raggiungimento, pianificando un opportuno insieme di attività infermieristiche sempre correlate al bisogno e un complementare insieme di rilevazioni dei parametri vitali.
Oltre alle attività assistenziali legate ai bisogni del paziente, le attività infermieristiche includono anche tutte le attività correlate (pre e post) all'intervento chirurgico e agli esami diagnostici ai quali è sottoposto il paziente, come, ad esempio, la compilazione di scale di valutazione, il completamento delle richieste esami diagnostici o prestazioni specialistiche prescritte dai clinici.
Il sistema deve consentire l'esecuzione delle attività infermieristiche che nascano preferibilmente in modalità automatica o per richiesta del medico (attività pre/post-operatorie, richiesta di esami strumentali/laboratorio, rilevazione parametri vitali, somministrazione farmaci) oppure tramite pianificazione manuale per altre tipologie di attività.
Il sistema di CCE deve consentire all'operatore di validare attività scaturite automaticamente dall'analisi dei bisogni, deve segnalare l'avvenuta o la mancata esecuzione di attività pianificate o eseguite in modalità estemporanea e deve visualizzare l'andamento delle attività svolte.

Funzionalità obbligatorie	Note/Dettaglio
Attività infermieristiche	*Le attività che compongono la worklist infermieristica riguardano le seguenti tipologie:* *- attività assistenziali legate ai bisogni del paziente* *- attività infermieristiche pre e post-operatorie o pre esame diagnostico* *- rilevazione parametri vitali* *- somministrazione dei farmaci (vedi anche paragrafo sul ciclo del farmaco)* *- compilazione di scale di valutazione e schede legate ai dispositivi medici* *- richieste d'esami di laboratorio previa prescrizione del medico e conseguente attività di prelievo ematico* *- richieste d'esami di altro genere previa prescrizione del medico* *- attività infermieristiche correlate alla gestione dei presidi e dei dispositivi*

Funzionalità obbligatorie	Note/Dettaglio
Attività infermieristiche	*Pianificazione Attività Infermieristiche* *Il sistema deve consentire la pianificazione delle attività infermieristiche compilando schede che includano tipologia di attività, descrizione, a quale ruolo assegnare l'attività e che presentino diversi indicatori di durata e frequenza di esecuzione della singola attività.* *Worklist per paziente* *Il sistema deve poter offrire per ciascun paziente la visualizzazione dell'elenco delle attività infermieristiche previste nel giorno, la loro descrizione, autore della pianificazione, dettaglio dell'attività opportunamente filtrabili per tipologia.* *Esecuzione delle attività* *L'operatore deve poter aprire l'elenco delle attività infermieristiche e per quelle eseguite deve poter impostare l'avvenuta esecuzione o la mancata esecuzione, aggiunta di note (obbligatoria per mancata esecuzione), inserimento di valori per parametri di interesse (bilancio idrico ad esempio), nascondere dalla worklist l'attività se completata nell'ambito della giornata.* *Andamento delle attività infermieristiche* *Il sistema deve poter offrire un riepilogo per paziente o per reparto per le attività pianificate, per le attività eseguite o non eseguite.* *Per quelle eseguite/non eseguite deve essere possibile vederne l'andamento nel tempo per paziente.*
Rilevazione parametri vitali	*Rappresenta il modello di funzionalità da adottare per consentire l'inserimento e la visualizzazione in formato tabellare e/o grafico (ove necessario) dei valori dei parametri vitali del paziente (temperatura, dati emodinamici, etc.), di tutte le rilevazioni cliniche specifiche (es. foglio emodinamica volumetrica, foglio respiratorio riassuntivo, bilancio idrico, ecc..), e delle rilevazioni del dolore (di raccordo con l'area delle valutazioni infermieristiche).* *Deve essere possibile consultare tutte le pianificazioni attive nella data e fascia oraria di interesse.* *Per ogni pianificazione deve essere possibile registrare l'avvenuta, o la mancata, rilevazione tramite caselle di spunta. I valori da rilevare possono essere multipli per parametro (ad esempio pressione arteriosa).* *In caso di mancata rilevazione deve essere possibile inserire un commento che motivi la mancata rilevazione e, se possibile, deve venir generata automaticamente una nota nel diario infermieristico che riporti utente, parametro vitale e commento dell'operatore.*

2.2.5 —— Ciclo del farmaco

La gestione della farmacoterapia rappresenta uno dei processi più importanti nell'ambito del Clinical Risk Management; il corrispondente modulo della Cartella Clinica Elettronica deve assicurare la tracciatura delle operazioni di prescrizione, allestimento/preparazione, somministrazione e consegna del farmaco e deve consentire la gestione sia della terapia farmacologica intesa come eventuale standard per tutte le unità operative (definito a livello aziendale), sia delle terapie farmacologiche tipiche delle singole specialità cliniche (ad esempio chemioterapie, terapie anticoagulanti, liquidi di contrasto, ecc.).
Il sistema dovrà supportare l'attività di prescrizione, somministrazione o consegna del farmaco al paziente in regime di ricovero ordinario (degenza), ricovero diurno (Day Hospital), alla dimissione dai suddetti regimi, ma anche in regime ambulatoriale. Per quanto riguarda la consegna dei farmaci è necessario prevedere anche la possibilità di consegna dei farmaci prescritti in reparto (o DH o Ambulatorio) direttamente in farmacia mediante opportune funzionalità o attraverso l'integrazione con sistemi terzi.

Funzionalità obbligatorie	Note/Dettaglio
Prescrizione terapia	*Il modulo deve consentire al medico di prescrivere un farmaco nelle diverse forme possibili di terapia:* *<u>Terapia non protocollata</u>* *- a orario standard, da ripetere fino alla data di sospensione con uno schema orario a scelta, a dose fissa o variabile alle diverse ore;* *- ad infusione continua, per terapie infusive in continuo per le quali il medico decide il dosaggio del farmaco per allestire il primo contenitore (sacca) e la velocità di infusione (con il supporto per il calcolo); nel decorso della terapia il medico potrà variare le velocità di infusione e gli infermieri potranno allestire tutti i contenitori necessari dei quali rimarrà tracciato, oltre all'attività di preparazione, anche l'orario e l'operatore della messa in somministrazione;* *- al bisogno, in cui le somministrazioni sono effettuate direttamente dal personale infermieristico, rispettando i dettagli ed i limiti indicati dal medico;* *- estemporanea, per la prescrizione di una singola somministrazione non programmata, estemporanea appunto.* *<u>Terapia protocollata</u>* *- protocolli chemioterapici, prescrizione di uno schema di terapia protocollata personalizzabile sul paziente.* *La selezione del farmaco deve avvenire tramite il prontuario, elenco dei farmaci disponibili in reparto e/o disponibili in ospedale oppure dal prontuario nazionale (tali elenchi devono essere aggiornati secondo la normativa vigente).* *Il sistema deve disporre di un archivio di protocolli standard (template) in formato strutturato, che in fase di prescrizione possono essere attualizzati, riconfigurati e validati sullo specifico caso clinico.*

Prescrizione terapia	*Inoltre, deve essere possibile creare profili preferenziali di terapia e, per ogni farmaco, una configurazione standard della prescrizione (per adulti/pediatrica/basata su parametri antropometrici del paziente), in modo che il sistema generi una proposta di prescrizione coerente facilitando l'attività prescrittiva.* *La selezione del/dei farmaco/i dovrebbe avvenire preferibilmente per principio attivo + forma farmaceutica + pezzatura/dosaggio oppure per brand commerciale o per protocollo, prevedendo tutte le modalità di selezione. La prescrizione deve riportare tutte le informazioni, dando tuttavia maggior evidenza al principio attivo.* *Il sistema deve poter gestire la prescrizione di quei farmaci che non sono inclusi nel catalogo di reparto e dei farmaci fuori indicazione (farmaci off-label).* *Deve essere possibile impostare sulla prescrizione, per ogni singolo farmaco, almeno le seguenti caratteristiche:* *- Modalità di somministrazione.* *- Farmaco e principio attivo (prodotto generico relativo), in conformità con le indicazioni aziendali circa la selezione del brand/commerciale o del principio attivo.* *- Forma farmaceutica (ricavata da prodotto generico relativo) e pezzatura.* *- Composizione con più farmaci in infusione (prescrizione preparati).* *- Numero di unità di somministrazione per ogni atto di somministrazione (dosaggio).* *- Eventuale unità antropometrica cui rapportarsi per calcolare la dose.* *- Numero delle somministrazioni al giorno o per intervallo di giorni (con giorni di somministrazione e con orari di somministrazione proposti automaticamente e possibilità di impostare un piano orario di somministrazione standard da parte del personale infermieristico).* *- Durata dell'infusione per farmaci iniettabili (ora inizio e ora fine).* *- Durata (data inizio e data fine) della terapia.* *- Campo note per il prescrittore (es. subordinazione della somministrazione a determinati eventi/sintomi/parametri).* *Il sistema deve eseguire controlli automatici su eventuali reazioni avverse/allergie del paziente, anche ad uno solo dei principi attivi selezionati dal medico e avvisare attraverso degli alert il rischio di evento avverso, tracciando l'informazione qualora il medico confermasse la sua selezione dopo l'avviso.* *Il sistema dovrebbe essere fornito di controlli automatici per:* *- Doppie prescrizioni per il medesimo paziente;* *- Allergie (sulla base del principio attivo presente all'ultimo livello della codifica ATC);* *- Dosaggi impropri;* *- Via di somministrazione improprie per farmaco prescritto;* *- Interazioni tra farmaci.* *Così come dovrebbe fornire anche funzionalità di calcolo per derivare la dose di farmaco a partire da parametri antropometrici (es. peso, altezza, superficie corporea, …) piuttosto che per calcolare la durata di un'infusione.* *Il sistema deve consentire l'inserimento/validazione di terapie in corso prima del ricovero, ponendo in adeguata evidenza l'indicazione di eventuali farmaci portati dal domicilio e gestendo delle modifiche/passaggio da brand commerciale a farmaco sostitutivo: questo di concerto con le funzionalità della CCE relative all'Inquadramento Clinico.*

Prescrizione terapia	*Deve essere possibile dalla visualizzazione di una terapia accedere rapidamente alla modifica della stessa. Il modulo per la gestione della prescrizione deve generare opportune segnalazioni all'area infermieristica ad ogni modifica della terapia impostata dal medico.* *Per alcune terapie farmacologiche deve esser possibile accedere ad informazioni necessarie alla prescrizione come ad esempio parametri vitali, risultati di esami di laboratorio come il tempo di protrombina per la prescrizione di farmaci anticoagulanti e l'andamento della glicemia per i farmaci per diabetici.* *Altre caratteristiche potrebbero essere:* *- Il sistema mostra tutte le terapie impostate sul paziente (attive o sospese) e lo storico delle modifiche di ciascuna di esse.* *- È possibile organizzare la prescrizione per tipologia di somministrazione.* *- È possibile trasformare la terapia ospedaliera in terapia di dimissione.* *- Il sistema permette la prescrizione di terapie in atto al momento dell'ingresso.* *- Il sistema consente la prescrizione di terapie e successiva somministrazione del farmaco a pazienti degenti o in Day Hospital.* *- Il sistema permette la gestione, coerentemente con le policy aziendali, di prescrizioni differite in caso di urgenze e prescrizioni autonome.* *- È possibile visualizzare lo stato sinottico delle prescrizioni.*
Somministrazione Terapia	*Nell'ambito del processo di farmacoterapia, la componente detta di somministrazione del farmaco deve avere come obiettivo quello di tracciare la corretta somministrazione della farmaco terapia al paziente consentita solo in presenza di una corrispondente prescrizione medica. Il sistema deve altresì permettere somministrazioni di urgenza, opportunamente segnalate.* *<u>Terapie da somministrare</u>* *Il sistema deve visualizzare tutte le farmacoterapie da somministrare al paziente raggruppate per data ora e turno infermieristico. Oltre alle terapie effettivamente prescritte per data e turno selezionati il sistema deve evidenziare in modo opportuno anche terapie antecedenti non ancora somministrate.* *Per ogni terapia deve essere possibile registrare l'avvenuta, o la mancata, somministrazione e in questo secondo caso l'operatore deve lasciare un commento che motivi la mancata somministrazione e un'opportuna segnalazione.* *<u>Somministrazione fuori orario</u>* *Se l'orario di prescrizione e quello di somministrazione per un tempo superiore ad un intervallo di tempo configurabile è opportuno venga chiesto all'infermiere di inserire un commento che motivi il ritardo generando un'opportuna segnalazione.* *<u>Terapie in corso (infusionali)</u>* *Per le terapie infusionali l'operatore deve poter indicare l'inizio della terapia, la sua conclusione e solo su prescrizione del medico il cambio di velocità dell'infusione o la sua sospensione e conseguente successivo riavvio.*

	<u>Andamento farmacoterapia</u> *Deve essere consentito a medici ed infermieri di visualizzare l'intero andamento delle farmacoterapie somministrate o meno al paziente corrente attraverso una sinossi delle terapie grafica o tabellare.* *Altre caratteristiche:* *- Il sistema deve presentare gli stessi controlli della fase di prescrizione per quanto attiene ad allergie, interazioni, ecc.* *- Il sistema deve tener traccia dell'avvenuta somministrazione e degli orari di inizio e fine somministrazione delle infusioni.* *- Il sistema deve poter segnalare le somministrazioni non eseguite, in scadenza.* *- Il sistema deve presentare degli alert in caso di discrepanze tra prescrizione e somministrazione (farmaco differente o non somministrato) e la possibilità di aggiungere annotazioni.* *- Il sistema deve supportare la programmazione infermieristica sulla preparazione della somministrazione tramite strumenti quali stampe e visualizzazioni configurabili.* *- Il sistema deve poter supportare tecnologie barcode per il riconoscimento di farmaco e paziente a supporto della somministrazione.* *- Il farmacista ospedaliero deve poter avere visibilità sulle terapie impostate sui pazienti (obbligatorio in caso di antiblastici) con la possibilità di inviare proposte alternative al prescrittore o bloccare la somministrazione in caso di pericolo.*

2.2.6 —— Ciclo operatorio e protesi

Il percorso operatorio di un paziente comincia normalmente con una prima visita ambulatoriale e si conclude con il follow up post intervento chirurgico. Nelle restanti situazioni il percorso operatorio può avere inizio con un accesso in emergenza da Pronto Soccorso ed il successivo trasferimento diretto in sala operatoria oppure può avere inizio come urgenza da reparto.

Le fasi previste per la gestione di un paziente chirurgico sono:

Gestione Preoperatoria:

- Visita Chirurgica
- Visita Anestesiologica
- Gestione Lista di Attesa
- Accertamenti Preoperatori
- Redazione Programma Operatorio

Gestione Intraoperatoria:

- Preparazione Sala Operatoria
- Identificazione Paziente
- Compilazione Cartellino Anestesiologico
- Redazione Verbale Operatorio

Gestione Post-Operatoria:

- Dimissione dal Blocco Operatorio

A supporto di queste fasi il sistema deve prevedere:

- moduli utilizzati in ambulatorio e in reparto per gestire tutte le fasi preliminari all'intervento
- moduli utilizzati all'interno del blocco operatorio per gestire le fasi dell'intervento
- moduli specifici per la pianificazione dell'allocazione delle Sale Operatorie ed il controllo delle attività di Sala
- un modulo per la redazione del Registro Operatorio di Sala e relativa stampa

Di seguito il dettaglio delle funzionalità sopra elencate.

Funzionalità obbligatorie	Note/Dettaglio
Gestione pre-operatoria: *visite pre-operatorie*	*La valutazione preoperatoria è la parte che tipicamente viene inclusa nell'ambito del perimetro della CCE mentre le altre funzionalità sono normalmente gestite con applicativi specifici/verticali di sala operatoria che, nel caso, si dovranno quindi integrare con la CCE (di minima acquisendo i dati rilevati in fase preoperatoria e inserendo in CCE il verbale operatorio).* *<u>Visita Chirurgica</u>: devono essere raccolte tutte le informazioni necessarie ad una valutazione generale del paziente. Ad esempio devono essere raccolte tutte le informazioni disponibili sull'Anamnesi (Familiare, Fisiologica, Patologica Remota, Farmacologica, Allergie ecc.) e l'Esame Obiettivo. Se il paziente necessita di intervento chirurgico viene compilato in questa fase il modulo di prenotazione e inserimento in lista di attesa. In tal caso, contestualmente alla visita chirurgica, vengono prescritti anche gli accertamenti pre-operatori necessari (è opportuno che sia supportata l'indicazione di protocolli preconfigurati).* *<u>Visita Anestesiologica</u>: viene normalmente prenotata come ultima fra gli accertamenti pre-operatori in modo tale da rendere disponibili all'anestesista tutti i risultati degli esami già richiesti dal chirurgo. Le informazioni già precedentemente registrate in sede di visita chirurgica devono poter essere ereditate in automatico durante la visita anestesiologica. In questa fase devono essere riviste e completate le informazioni sull'Anamnesi e l'Esame Obiettivo. Vengono registrate le indicazioni pre-operatorie (es: profilassi antibiotica), eventuali depositi necessari, eventuale preanestesia, l'anestesia, eventuali ulteriori accertamenti da effettuare e vengono infine compilate le Conclusioni Anestesiologiche con le quali l'anestesista dichiara le condizioni operatorie del paziente.* *In questa fase preoperatoria deve essere prevista la raccolta del Consenso Informato.*
Gestione pre-operatoria: *liste di attesa e programma operatorio*	*I Pazienti per i quali si rende necessaria una Procedura Chirurgica devono essere inseriti in **Lista di Attesa** (tipicamente contestualmente o dopo la visita chirurgica che determina la necessità dell'intervento).* *Per gestire le liste di attesa è necessario uno strumento che consenta di:* *- Valutare la totalità degli Interventi Chirurgici da effettuare suddivisi per Unità Operativa, Agenda, Tipo di intervento, ecc.* *- Prenotare gli accertamenti pre-operatori richiesti in fase di Visita Chirurgica o Anestesiologica* *- Controllare l'effettiva esecuzione dei pre-operatori al momento del ritorno dei referti* *- Concordare la Data di Ricovero dopo la conferma di idoneità a sostenere l'intervento da parte del personale medico (in particolare da parte dell'anestesista)*

	- Gestire eventuali variazioni rispetto alla data concordata (indisponibilità del posto letto, indisponibilità del paziente, ecc.) *Pianificare l'attività di sala (vedi "Pianificazione Sale Operatorie") sulla base della programmazione della singola sala o del blocco operatorio.* *- Redigere e stampare il **Programma Operatorio** che viene poi consegnato ai relativi responsabili di blocco per la preparazione delle Sale Operatorie (vedi anche punto seguente "Preparazione della Sala Operatoria"). Il programma operatorio viene definito incrociando le priorità in lista di attesa con la pianificazione delle sale operatorie.*
***Gestione intra-operatoria**:* *Preparazione della Sala Operatoria*	*Per la preparazione della Sala, a disposizione del personale di Blocco, il **Programma Operatorio** deve racchiudere tutte le informazioni necessarie a preparare il materiale richiesto all'esecuzione dell'intervento chirurgico (lista pazienti del giorno per ogni sala operatoria, tipo di intervento, eventuali allergie al lattice, lateralità, equipe coinvolta, ecc.).*
***Gestione intra-operatoria**:* *Accettazione in sala operatoria*	*Il paziente deve essere identificato (**Accettazione in sala operatoria**) dal personale medico prima di avviare la procedura chirurgica (ad esempio grazie all'utilizzo di un lettore di barcode).*
***Gestione intra-operatoria**:* *Check list*	*Gli operatori sanitari, mediante l'utilizzo di "**check list**" per la sicurezza del paziente chirurgico, verificano attività (identificazione paziente, preparazione del paziente, tipo d'intervento da eseguire ecc.), strumenti, materiali e quant'altro necessario per l'esecuzione dell'intervento chirurgico.* *"**Check list**" di verifica devono obbligatoriamente essere utilizzate in tre momenti specifici della fase intraoperatoria:* *- "check-in", verifiche da effettuare quando il paziente entra in sala operatoria prima dell'anestesia* *- "time-out", verifiche da effettuare da parte dell'intera equipe di sala, a paziente già sedato, prima dell'incisione* *- "sign out", verifiche da effettuare prima della dimissione del paziente, ancora sedato, dalla sala.*
***Gestione intra-operatoria**:* *Cartellino Anestesiologico*	*Durante la procedura chirurgica l'anestesista deve poter registrare, in tempo reale, le informazioni di seguito elencate (**Cartellino Anestesiologico**):* *- i dati generali dell'intervento: effetto della preanestesia, tipo di anestesia, posizione del paziente ed eventuali cambi di posizione effettuati, presidi utilizzati, tipo di ventilazione, operatori ed altro personale, eventuali complicanze;* *- tempi di sala: si ricordi che i tempi standard che devono essere obbligatoriamente registrati nella fase intra-operatoria sono i tempi di ingresso in sala, ok anestesista (Time out), inizio e fine dell'intervento chirurgico, uscita dalla sala (tempi che devono obbligatoriamente comparire nel verbale operatorio)* *- l'anestesia: farmaci, infusioni, gas anestetici somministrati* *- i parametri vitali del paziente durante l'intervento, alcuni dei quali possono essere acquisiti automaticamente dalla strumentazione di Sala Operatoria.*
***Gestione intra-operatoria**:* *Order entry*	*Integrazione con il sistema di gestione richieste verso i servizi diagnostici (es.: Laboratorio, Radiologia, Anatomia Patologica).*

***Gestione intra-operatoria**:* *Verbale operatorio*	*Al termine della procedura chirurgica il sistema deve consentire la compilazione del **Verbale Operatorio**, consentendo altresì di ereditare dalle precedenti fasi del percorso chirurgico i dati già disponibili (i dati paziente inseriti nell'ambito della visita chirurgica quali eventuali Allergie, Terapia Farmacologica in atto, etc. e durante la visita anestesiologica ed i tempi di sala registrati dall'anestesista durante la compilazione del cartellino anestesiologico).* *I contenuti essenziali del verbale operatorio sono i seguenti:* *- Dati identificativi del paziente* *- Sito chirurgico e lateralità* *- Diagnosi pre-operatoria, diagnosi intra-operatoria* *- Indicazione della procedura programmata* *- Data, ora di inizio e ora di fine dell'atto operatorio* *- Nome del primo operatore e di quanti hanno partecipato direttamente all'intervento (indicazione di equipe supplementari nel caso partecipino più equipe)* *- Diagnosi finale e denominazione della procedura eseguita (classificate secondo codifica es.: ICD-IX CM)* *- Tipo di anestesia utilizzata e nome dei sanitari che l'hanno condotta* *- Descrizione chiara e sufficientemente particolareggiata della procedura attuata e relativa codifica della procedura* *- Protesi, materiali ed eventuali procedure trasfusionali eseguite* *- Sottoscrizione da parte del primo operatore* *- Numero del verbale* *- Numero identificativo del ricovero del paziente* *- Unita operativa chirurgica* *- Unita operativa di ricovero del paziente* *- Codifica delle procedure eseguite, in funzione della compilazione della SDO* *- Tempi operatori (ingresso in sala, ok anestesista, inizio e fine dell'intervento chirurgico, uscita dalla sala)* *Al termine della compilazione del verbale, il primo Operatore dell'equipe chirurgica, o un utente autorizzato, effettua la convalida definitiva del documento, che comporta il blocco di tutti i campi e la creazione di un documento definitivo.*
Gestione post-operatoria: *Monitoraggio in Sala Risveglio*	*È opportuno che la registrazione dei dati clinici del paziente sia garantita, senza soluzione di continuità, anche durante il risveglio sia da parte dell'anestesista (tempi di risveglio) sia da parte del personale infermieristico (parametri vitali del paziente eventualmente acquisiti automaticamente dalla strumentazione al posto letto).*
Gestione post-operatoria: *Valutazione post-operatoria*	*All'atto della dimissione dal blocco operatorio viene redatto un documento che attesta le condizioni del paziente e che accompagna lo stesso nel suo rientro al reparto di degenza.* *La Valutazione Post-operatoria deve indicare:* *- Le condizioni (respiratorie, cardiocircolatorie, neurologiche) del paziente* *- Il tipo di sorveglianza necessaria nel post operatorio* *- La segnalazione degli accessi vascolari e di altri mezzi invasivi presenti e il loro stato* *- Le terapie in corso e quelle consigliate nel post operatorio* *- Gli esami di controllo necessari ed i parametri da monitorare* *- Ora/minuti della dimissione dal blocco operatorio, o da diverso ambiente di intervento, e trasferimento al reparto di degenza.*

Pianificazione Sale Operatorie	*Il modulo di Pianificazione delle Sale permette di allocare l'utilizzo delle Sale Operatorie alle diverse chirurgie.* *Il modulo assolve principalmente alla necessità di Programmare un piano di utilizzo delle Sale Operatorie per ogni Unità Operativa.* *Ogni Sala Operatoria deve disporre di un'**agenda** configurabile in termini di orari di servizio e tipologia dell'attività chirurgica svolta.* *È utile poter pre-configurare o impostare giorno per giorno eventuali segnalazioni su specifiche da osservare nell'organizzazione della singola sala (es. manutenzione programmata, indisponibilità della sala, ecc.).*
Registro operatorio	*L'insieme degli atti operatori (verbali) convalidati va a comporre il registro di sala che, nella sua gestione elettronica, deve essere corredato delle opportune funzionalità di stampa.*

2.2.6.1 Gestione presidi medico-chirurgici (dispositivi e protesi)

Funzionalità obbligatorie	Note/Dettaglio
Annotare e gestire le attività relative a presidi medico-chirurgici	*Possibilità di annotare le attività di gestione dei dispositivi/mezzi invasivi effettuate dal personale clinico sul paziente.* *Possibilità di utilizzare codifiche specifiche (es. nomenclatore dispositivi e protesi).* *Possibilità di gestire le attività specifiche di medici (prescrizione o esecuzione) e infermieri (esecuzione) es.: inserimento, medicazione, lavaggio, rimozione.*

2.2.6.2 Tracciabilità dei ferri chirurgici e dei presidi medico-chirurgici

La tracciabilità dei ferri chirurgici e dei presidi medico chirurgici deve garantire, durante l'intero ciclo di sterilizzazione dello strumento (utilizzo, pre-disinfezione, pulizia, disinfezione, controllo, condizionamento, sterilizzazione, trasporto, stoccaggio, utilizzo), di poter:

- tracciare lo strumento in modo semplice e veloce
- ricomporre correttamente i kit chirurgici
- associare lo strumento alla seduta operatoria e/o al paziente
- programmare le sedute operatorie e gli inserimenti/applicazioni dei presidi medico-chirurgici senza rischiare di non avere lo strumento necessario
- avere dei kit chirurgici ottimizzati per il tipo di operazione

Esistono sistemi di tracciabilità completamente manuali ed altri informatizzati supportati da software per il riconoscimento del singolo ferro chirurgico o dispositivo.

2.2.7 —— Order entry

L'order entry gestisce il flusso di richieste di prestazioni dai reparti e servizi ospedalieri richiedenti verso i servizi erogatori e le relative informazioni di ritorno (dati sulle prestazioni erogate, referti, immagini, allegati), favorendo una gestione paperless e filmless del flusso diagnostico tra reparti e servizi erogatori e consentendo un eventuale controllo dell'appropriatezza delle richieste effettuate.

Funzionalità obbligatorie	Note/Dettaglio
Inserimento ordini	*L'order entry deve permettere di:* *- poter effettuare richieste verso i servizi destinatari;* *- poter effettuare prenotazioni dirette verso i servizi che mettono a disposizione delle agende prenotabili.* *La scelta fra le proposte sopra descritte può dipendere dall'organizzazione dell'ospedale e da quella del servizio erogatore. Per esempio il servizio di radiologia può mettere a disposizione agende prenotabili direttamente dai reparti di degenza.* *Ogni reparto deve poter essere configurato per:* *- richiedere a determinati servizi (per soddisfare alle esigenze del tipo: solo il reparto A può effettuare prenotazione verso la radiologia; solo i reparti A e B possono richiedere alla cardiologia dell'ospedale X mentre gli altri devono richiedere alla cardiologia dell'ospedale Y,…);* *- richiedere solo certe prestazioni e queste devono poter essere differenziate per regime (urgenza e routine);* *- permettere l'inserimento di una determinata tipologia di richiesta solo a personale specializzato (es. le richieste verso la radiologia devono essere inserite solo da utenti medici).*
Gestione ordini	*Gli utenti devono poter visionare lo stato d'avanzamento delle richieste.* *Per certe tipologie di richieste, per esempio quelle in vitro e/o richieste di emocomponenti, devono poter stampare le etichette, poter visionare i dati strutturati ed i referti (parziali e totali). Nel caso di esami strumentali, l'utente deve anche poter vedere le immagini prodotte a fronte della richiesta.*
Visualizzazione documenti	*Deve essere data la possibilità di visionare i referti che afferiscono ad ogni ordine.* *La visualizzazione dei referti può essere anche effettuata a livello di paziente.*

2.2.8 —— Fase di dimissione

Nella fase di dimissione deve essere redatto un documento riepilogativo e conclusivo del contatto con la struttura ospedaliera.

I documenti che si devono poter compilare e firmare sono:

- lettera di dimissione (del ricovero ordinario o DH);
- lettera di trasferimento (solo nel caso di dimissione verso altri reparti);
- lettera per la terapia domiciliare (DH): ad ogni accesso il medico deve poter indicare al paziente la terapia da seguire a casa;
- lettera al medico curante (DH): ad ogni accesso può essere necessario far avere al medico di base la situazione del paziente;
- lettera di prosecuzione di ricovero;
- lettera di dimissione infermieristica;
- eventuale integrazione della lettera di dimissione (ad es. nel caso di recipimento ex post di esiti di esami di anatomia patologica).

La lettera può essere automaticamente compilata nelle sezioni che richiedono di riportare azioni che sono state memorizzate in altri punti della cartella di ricovero (per esempio: motivo del ricovero, accertamenti eseguiti).

Deve essere previsto un aiuto alla compilazione ovvero, fornire all'utente la possibilità di avere "sotto mano" i punti salienti del ricovero che lo aiutino a compilare la lettera: elenco richieste avvenuto durante il periodo di degenza, elenco referti, informazioni dell'anamnesi e dell'esame obiettivo.

Funzionalità obbligatorie	Note/Dettaglio
Lettera di dimissione	*Le informazioni fondamentali da inserire nella lettera di dimissione secondo lo standard Joint Commission e il Manuale della Cartella Clinica sono le seguenti:* *- Motivo del ricovero* *- Anamnesi, diagnosi e problemi (risolti e non risolti al momento della dimissione) / Epicrisi medica* *- Diagnosi di dimissione* *- Data e ora di chiusura, medico di dimissione* *- Accertamenti eseguiti* *- Trattamenti e/o altre procedure eseguite* *- Terapia farmacologia attuata* *- Terapia suggerita alla dimissione* *- Presidi prescritti alla dimissione* *- Istruzioni di follow-up* *- Eventuali occorrenze di prestazioni sanitarie e/o sociali, da richiedere alle strutture esterne (es. RSA, ADI,..) in termini di continuità assistenziale* *- Suggerimenti su abitudini di vita (es. regime alimentare, attività fisica, ecc.)* *Sono parti integranti del documento le Comunicazioni infermieristiche alla dimissione, relativamente ad esempio ai bisogni di assistenza infermieristica aperti alla dimissione, le valutazioni del dolore, le lesioni da pressione non ancora risolte, i dispositivi eventualmente presenti, i suggerimenti per il follow-up.*
Lettera di trasferimento	*Il trasferimento interno, da un'unità operativa ad altre dello stesso ente erogatore, deve essere corredato da un foglio di trasferimento che relazioni i problemi clinici salienti, descriva le modalità dell'assistenza medica ed infermieristica in essere ed espliciti i motivi del trasferimento stesso. In genere sono da indicarsi, ad esempio:* *- Per la componente medica: motivo del ricovero, accertamenti significativi effettuati o in corso, diagnosi formulate, procedure eseguite o in corso, terapie farmacologiche effettuate, in corso o prescritte, condizioni del paziente e diagnosi alla dimissione;* *- Per la componente infermieristica: bisogni di assistenza infermieristica aperti (con relative finalità assistenziali e dettaglio), procedure eseguite o in corso (es. dispositivi), valutazioni infermieristiche, valutazioni del dolore, lesioni da pressione non ancora risolte.* *Nella forma più elementare, la compilazione dei fogli di trasferimento deve essere supportata con l'indicazione automatica delle informazioni anagrafiche, importando in campi tematici, formattabili, e codificati/strutturati in sezioni le informazioni essenziali che costituiscono i fogli clinici ordinari, fornendo al medico possibilità di integrare quanto importato. Le sezioni previste sono:* *- Anamnesi, diagnosi e problemi (inclusa la codifica della diagnosi principale);*
	- Epicrisi medica; *- Terapia in corso.* *Analogamente deve poter avvenire per la parte infermieristica, con la possibilità di importare ed integrare quanto inserito nella documentazione clinica compilata durante la degenza (vedi sezione 4.5.5), in particolare l'informazione deve essere strutturata per quanto riguarda:* *- lo stato dei BAI infermieristici.* *Per queste quattro aree è richiesta una gestione evoluta della compilazione area per area con maschere dedicate di compilazione strutturata, precompilate sulla base delle informazioni disponibili nei fogli clinici di riferimento.*
Lettera per la terapia domiciliare del DH	*Le informazioni fondamentali sono:* *- terapia domiciliare (contenente l'elenco dei farmaci, la posologia e la durata);* *- indicazioni dei farmaci da ritirare presso la farmacia ospedaliera.*
Lettera al medico MMG-PLS	*Le informazioni fondamentali da inserire nella lettera al MMG-PLS sono le seguenti:* *- decorso clinico* *- accertamenti eseguiti* *- trattamenti e/o altre procedura eseguite* *- terapia domiciliare* *- primo ciclo* *Il medico del DH può decidere se ad ogni accesso redigere la lettera per la terapia domiciliare oppure la lettera al MMG-PLS che ha inglobata la terapia che deve essere seguita a casa dal paziente.*
Lettera di prosecuzione di ricovero	*Le informazioni fondamentali da inserire nella lettera di prosecuzione di ricovero sono:* *- accertamenti eseguiti* *- trattamenti e/o altre procedure eseguite* *- terapia domiciliare* *- follow up* *- relazioni conclusiva* *La parte di supporto alla compilazione dovrà far vedere solo le informazioni dalla data di dimissione in avanti.* *La compilazione della lettera di prosecuzione di ricovero può essere effettuata entro il tempo previsto per l'archiviazione della cartella.*
Chiusura cartella	*È da prevedere una funzione di chiusura della CCE con firma elettronica dell'intera CCE e dell'indice dei documenti che la compongono.*

2.2.9 —— Ciclo ambulatoriale

È stato dedicato un breve paragrafo al ciclo ambulatoriale in quanto con una certa frequenza, nella prassi, un ricovero viene generato da un evento ambulatoriale, durante un ricovero vengono richieste ed effettuate attività ambulatoriali e spesso dopo il ricovero vengono effettuate attività di follow-up a completamento dello stesso.

Funzionalità obbligatorie	Note/Dettaglio
Inquadramento ambulatoriale	*L'inquadramento ambulatoriale comprende la valutazione di fattori fisici/funzionali, psicologici, sociali ed economici per identificare il motivo della richiesta di visita ambulatoriale in ottica dei successivi passi per la formulazione della diagnosi, prescrizione di esami e predisposizione di una terapia.* *Comprende:* *- Motivo della visita / Quesito diagnostico.* *- Sintesi Anamnestica: tale sintesi puo essere eventualmente strutturata in anamnesi familiare, personale remota e recente.* *- Esame obiettivo e specialistico: costituisce anch'esso parte della valutazione d'ingresso e deve essere orientato all'esame dei diversi sistemi/apparati, specie di quelli correlati con le motivazioni della visita specialistica (ad es. Esame Obiettivo Muscolare nella Miastenia).* *- Elenco dei problemi attivi del paziente.* *- Terapie in corso.* *- Intolleranze alimentari, a farmaci, a sostanze e allergie.*
Trattamento ambulatoriale	*Durante la compilazione di un referto ambulatoriale deve essere data la possibilità di vedere i referti precedenti del paziente per poter effettuare i dovuto controlli (se necessario).* *Oltre ai referti precedenti può essere data la possibilità di vedere precedenti anamnesi, esami obiettivi e terapie farmacologiche.*
Refertazione ambulatoriale	*- Diagnosi / Conclusioni e indirizzo terapeutico* *- Eventuali prescrizioni (RUR)*

In questo paragrafo vengono indicate quelle funzionalità di un sistema di CCE che hanno valenza trasversale e che vengono, in ogni caso, ritenute come funzioni "minime" che devono essere garantite.

Funzionalità obbligatorie	Note/Dettaglio
Gestione di frasi standard come supporto alla compilazione a livello del singolo utente o di specialità, pervasiva a livello di tutto il sistema	*Questo permette di creare e condividere uno stesso dizionario a livello di azienda sanitaria.*
Gestione Notifiche e Allarmi	*Deve essere possibile disporre di un sistema di messaggistica che consenta di esporre warning per il team medico-infermieristico.*
Il sistema permette la visualizzazione di un piano di lavoro medico e infermieristico trasversale a tutte le azioni da effettuare sul paziente (Somministrazioni, Attivita infermieristiche assistenziali, Rilevazioni parametri da evadere)	*Questo permette di creare e condividere uno stesso dizionario a livello di azienda sanitaria.*
Il sistema dispone di una funzione di controllo che impedisca che un documento sia chiuso in presenza di campi tematici obbligatori non compilati	*Questo permette di creare e condividere uno stesso dizionario a livello di azienda sanitaria.*

Percorsi clinici	*Il sistema di CCE deve permettere in fase di dimissione ed in ogni istante precedente la refertazione che il sanitario possa associare l'episodio in corso a un dato percorso (esistente o nuovo).* *I possibili criteri di raggruppamento devono essere stabiliti a livello aziendale, e riguardano ad es. per patologia (es. diagnosi codificata ICD9-CM/ICD-10), per problema (es. ICD9-CM/ICD-10), per specialità, o in base ad altre codifiche riconosciute a livello regionale, nazionale, internazionale. Se l'episodio non è associato ad alcun percorso, costituirà un elemento a sé.*
Gestione Stato dei documenti	*Es.: il sistema permette la gestione della lettera di dimissione (forma di bozza) anche nei giorni precedenti la dimissione effettiva e la stesura di una possibile successiva versione integrativa (solo aggiunta di nuovi contenuti).*
*Visualizzazione dell'**ubicazione** fisica del paziente*	*All'interno dello strumento di gestione di CCE deve essere possibile visualizzare graficamente il layout del reparto con la visualizzazione chiara dei dati del paziente per ogni letto.*
*Il sistema deve consentire la gestione del paziente in formato **anonimo***	

3 —— CCE: compliance, sicurezza, valore documentale della CCE e problematiche relative alla sua corretta redazione e conservazione

3.1 —— Premessa

Nei due capitoli precedenti sono stati definiti tutti gli aspetti relativi all'implementazione della CCE intesa quale "**sistema informatico integrato aziendale**" finalizzato non solo a fornire un'adeguata base informativa sullo stato di salute del paziente, sui trattamenti effettuati e i risultati conseguiti, ma anche a facilitare l'integrazione operativa dei diversi professionisti sanitari che intervengono nell'ambito del processo diagnostico-terapeutico, in modo da favorire decisioni clinico-assistenziali appropriate e garantire la necessaria continuità delle cure al paziente stesso.

Oltre alle predette due fondamentali funzioni, le linee guida della Joint Commission International prevedono che la CCE debba anche "supportare la protezione legale degli interessi del paziente, dei medici e dell'azienda sanitaria, attraverso il tracciamento di tutte le attività svolte per permettere di risalire (rintracciabilità) ai responsabili, alla cronologia e alle modalità di esecuzione".

Ciò significa che qualsiasi progetto di implementazione di una CCE non può non porsi anche l'obiettivo che la stessa sia in grado di sostituire a tutti gli effetti, compresi quelli giuridico-probatori, la cartella clinica cartacea.

Questo capitolo fornisce una serie di considerazioni e raccomandazioni in tal senso, e tiene in conto:

- quanto si deve fare per necessità di compliance a leggi, norme e regolamenti (la CCE risente fortemente della delicatezza del dato da trattare e quindi della legge della Privacy e gli specifici provvedimenti del Garante della Privacy e del Codice di Amministrazione Digitale)
- quanto si può fare per implementare le più efficienti soluzioni (come ad esempio, per quanto riguarda l'integrità, la disponibilità e la riservatezza dei dati, l'autenticazione, la continuità operativa)
- quanto è necessario perché la cartella clinica elettronica fornisca almeno le stesse garanzie di quella cartacea in termini di correttezza e completezza dei dati, indispensabile per tutelare la salute dei pazienti ai quali si riferisce (come ad es. il valore documentale della CCE, firme elettroniche, conservazione). In questa parte vengono definite le modalità e gli accorgimenti che devono essere adottati per poter correttamente redigere e conservare la CCE intesa come documento informatico, ovvero come "rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti" [3].

Considerato, inoltre, che le attività di redazione, conservazione e consultazione della CCE, rappresentano di fatto operazioni di trattamento dei dati personali del paziente e, in particolare, di quelli idonei a rivelare il suo stato di salute, si ritiene indispensabile, dopo aver esaminato gli obblighi introdotti dalla vigente normativa in materia di protezione dei dati personali, di cui al D.Lgs. 196/03, e da altri provvedimenti del Garante Privacy in materia di trattamento di dati sanitari, evidenziare le misure di sicurezza che devono essere adottate in

[3] Art. 1, comma 1°, lett. p) del Codice dell'amministrazione digitale, di cui al D.Lgs. 82/2005, come modificato dal D.Lgs. 235/2010.

modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali del paziente contenuti nella CCE, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

È opportuno precisare comunque che in questo capitolo si farà riferimento solo agli aspetti informatici della sicurezza, o agli aspetti procedurali e di gestione focalizzati sulla sicurezza informatica in senso stretto.

Questo, ovviamente, non toglie che la sicurezza della CCE non possa essere assicurata con i soli strumenti informatici, ma dipenda anche da importanti aspetti organizzativo-gestionali e procedurali. In questo capitolo si farà riferimento ai soli aspetti dei requisiti, della gestione e delle tecnologie di sicurezza che presentano una qualche specificità nell'ambito della CCE: è chiaro ad esempio che anche i sistemi coinvolti nella gestione o nell'accesso alla CCE devono essere tutelati dal malware, ma sotto questo aspetto la CCE non presenta alcuna specificità, se non naturalmente l'ampio trattamento di dati sensibili, con quanto ciò comporta in termini di rischio e conformità alle normative. Da questo punto di vista appare utile ricordare che lo standard ISO 27799 "Health informatics - Information security management in health using ISO/IEC 27002" integra le indicazioni dello standard ISO/IEC 27002 in riferimento all'ambito sanitario.

3.2 —— Compliance della CCE

Le fonti normative principali in ambito sanitario sono riportati nell'elenco seguente.

- Decreto legislativo 196/2003 - Codice per la Protezione dei Dati Personali
  Linee guida in tema di Fascicolo Sanitario Elettronico (FSE) e dossier sanitario - Garante per la protezione dei dati personali -16 luglio 2009
- Prescrizioni in tema di Fascicolo Sanitario Elettronico (FSE) - Garante per la protezione dei dati personali 16 luglio 2009
- Linee guida in tema di referti on-line - Garante per la protezione dei dati personali - 19 novembre 2009
- Linee guida nazionali sul Fascicolo Sanitario Elettronico - Ministero della Salute - 11 novembre 2010
- Disegno di legge N. 2935 approvato dalla Camera il 28/09/2011 e trasmesso al Senato - Delega al Governo per il riassetto della normativa in materia di sperimentazione clinica e per la riforma degli ordini delle professioni sanitarie, nonché disposizioni in materia sanitaria
- Codice dell'Amministrazione Digitale D. Lgs. 30 dicembre 2010 n°235 che integra e modifica il precedente D. Lgs. n°82/2005

Il tema della compliance legale richiederebbe un approfondimento che non può essere esaurito in poche pagine. Ciò premesso, si ritiene importante focalizzare l'attenzione su alcune considerazioni di carattere generale:

- Di norma la legislazione non declina dettagliatamente le misure di sicurezza ma rimanda ad allegati tecnici (es. allegato B del Codice Privacy e Linee Guida interpretative di DigitPA) e a best practice internazionali (es.

ISO27000). Questo doppio passaggio comporta la necessità di una maggiore attenzione in fase di pianificazione e implementazione dei sistemi di CCE. La stretta interconnessione tra gestione della sicurezza e normativa sulla Privacy viene ulteriormente rafforzata dal testo del D.Lgs 196/03 laddove vengono introdotti i principi di "adozione di idonee e preventive misure di sicurezza" (art. 31) e di "adozione di misure minime di sicurezza" (art. 33) a loro volta dettagliatamente descritte nell'Allegato B dello stesso Decreto. Se da un punto di vista tecnico l'adozione di una misura di sicurezza, sia essa minima o idonea, è assolutamente necessaria qualora sia attuabile, da un punto di vista giuridico la distinzione tra le due è rilevante: la mancata adozione di misure minime di sicurezza determina delle responsabilità di tipo penale[4], mentre l'omissione di misure idonee determina un obbligo risarcitorio di cui all'art. 2050 del Codice Civile, ai sensi dell'art.15 del D.Lgs.196/03. In proposito va precisato che lo stesso art. 31 sancisce in modo abbastanza chiaro cosa si debba intendere per misure idonee: ogni qualsiasi intervento che sarebbe stato possibile adottare in ragione al "progresso tecnico (stato dell'arte del mercato tecnologico), alla natura dei dati oggetto del trattamento, alle specifiche caratteristiche del trattamento (con sistemi informativi o meno)" al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità del trattamento. Questa netta distinzione suggerisce un approccio alla sicurezza e alla privacy che richiede maggiori attenzioni nella definizione delle "migliori pratiche possibili" tra vincoli normativi e evoluzione della tecnologia al fine di contemperare un utilizzo sempre maggiormente esteso delle tecnologie informatiche e la privacy dei cittadini. Pone quindi ex ante un principio di massima cautela nella gestione di problematiche che appaiono particolarmente articolate e complesse (Perri, 2007).[5]

Misure Minime

- Definite per legge
- Art. 33-36 196/03 ed allegato B
- Modificabili per legge dal Ministero della Giustizia in accordo con semplificazione ed economia
- Rilevanza penale e amministrativa
- Maggiore staticità

Misure idonee

- Definite dal cliente in funzione del rischio
- Modificate nel tempo in funzione del mutato contesto del progresso tecnologico
- Rilevanza civilistica
- Maggiore difficoltà d'implementazione

- La complessità delle tematiche e le best practice richiedono che le misure di sicurezza siano definite in funzione di un'analisi del rischio che tenga conto della qualità, dell'importanza del dato trattato e dell'evoluzione delle tecnologie. Di conseguenza, per gli aspetti di compliance e di sicurezza, un progetto di implementazione di CCE deve prevedere l'interazione di diverse competenze: legale, sicurezza e rischio, tecnologica, organizzativa, qualità.
- Nei progetti di CCE rivestono uguale importanza la disponibilità del dato, la riservatezza e l'integrità, argomenti che verranno trattati successivamente. Nei fatti tutti questi aspetti sono il cuore della ISO27000 e sono presenti sia nella legge sulla Privacy sia nel testo del Codice dell'Amministrazione Digitale (citato). Analogamente alcune opportunità date dal progresso tecnologico, in particolare "Cloud e Mobile" richiedono, rispetto alla Sicurezza e alla Privacy, un'ulteriore attenzione per la quale raccomandiamo un approccio strutturato di adozione.

[4] Cfr. primo comma, art 169, D.Lgs 196/03 "chiunque essendovi tenuto, omette di adottare le misure minime previste dall'art. 13 è punito con l'arresto sino a 2 anni o con l'ammenda da diecimila a cinquantamila euro".
[5] Perri P., (2007), Privacy, Diritto e Sicurezza Informatica, Giuffrè, Milano

		Crittografia / cifratura			
Codice	**Industry**	**Dati**	**Dati (2)**	**Trasmissione**	**Trasmissione (2)**
Allegato B. Disciplinare tecnico in materia di misure minime di sicurezza	All	Stato di salute e vita sessuale (19.8)	Dati generici (24)		
Provvedimento in materia di videosorveglianza – 8 aprile 2010	All			Immagini via rete pubblica (3.3.1. lettera f)	
CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI	Sanità	Stato di salute e vita sessuale (Art.34, comma 1, lettera h)	Dati sensibili e giudiziari (Art.22, comma 6)		
Linee guida in tema di referti on-line – 19 novembre 2009	Sanità	Identità genetica (Art.6)		Consultazione referto online (Art.6 scenario 1 punto 1)	Invio referto tramite posta (Art.6 scenario 2 punto 2)
Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario – 16 luglio 2009	Sanità	Crittografia filesystem e database (Art.10)	Stato di salute e vita sessuale (Art.10)	Comunicazione elettronica del FSE tra titolari (Art.10)	
Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali – 24 luglio 2008	Sanità	Crittografia filesystem e database (Art.12 lettera a)		Protocolli di comunicazione (Art.12 lettera b)	
Aids: vanno rafforzate garanzie e misure di sicurezza sui dati sanitari	Sanità	Cifratura e separazione dati persone sieropositive o con AIDS			

3.2.1 —— Natura giuridica della cartella clinica

La cartella clinica, nonostante l'evidente rilevanza rivestita, non è disciplinata nel nostro ordinamento in maniera diretta e positiva. Per definirne la natura ed inquadrarne le implicazioni giuridiche in caso di illegittimi comportamenti da parte dell'estensore è necessario, quindi, fare riferimento alla dottrina e alla giurisprudenza.
Secondo alcuni autori la cartella clinica è un documento essenziale ed indefettibile in quanto rappresenta l'insieme dei dati relativi al paziente raccolti dal personale sanitario. Essa, pertanto, costituisce il presupposto indispensabile di qualsiasi prestazione sanitaria che non presenti carattere di mera episodicità, ma che si svolga secondo requisiti di continuità e di durata, consentendo la raccolta e l'integrazione dei dati anamnestici, degli elementi obiettivi, delle informazioni relative al decorso della malattia, e di ogni elemento di ordine diagnostico, prognostico o terapeutico, ordinati cronologicamente.
In dottrina la cartella clinica è considerata, inoltre, un essenziale strumento per consentire al paziente di avere adeguata e doverosa informazione in merito al suo stato di salute, alla diagnosi, alla cura della sua malattia, in maniera da permettergli scelte consapevoli, sicché questa deve essere chiara, leggibile e contenere tutte le informazioni indispensabili.
Dottrina e giurisprudenza si sono a lungo interrogate sulla natura della cartella clinica e l'orientamento prevalente della Cassazione penale ritiene che sia un atto pubblico, con tutte le conseguenze riconducibili alla violazione degli artt. 476 e 479 c.p.[6]
Analoga rilevanza è pure riconosciuta alla cartella clinica tenuta dalle case di cura convenzionate, in virtù del principio della delega di pubbliche funzioni conferita a soggetti privati dal Servizio Sanitario Nazionale (Cass. pen. 27.3.1992, sez. un.).

[6] Gli articoli 476 e 479 del codice penale riguardano rispettivamente il reato di falsità materiale e il reato di falsità ideologica.

La Cassazione penale ha più volte rilevato che "*la cartella clinica redatta da un medico di un ospedale pubblico è caratterizzata dalla produttività di effetti incidenti su situazioni giuridiche soggettive di rilevanza pubblicistica, nonchè dalla documentazione di attività compiute dal pubblico ufficiale che ne assume la paternità: trattasi di atto pubblico che esplica la funzione di diario del decorso della malattia e di altri fatti clinici rilevanti, sicchè i fatti devono esservi annotati contestualmente al loro verificarsi. Ne deriva che tutte le modifiche, le aggiunte, le alterazioni e le cancellazioni integrano il reato di falsità in atto pubblico, punibili in quanto tali; nè rileva l'intento che muove l'agente, atteso che le fattispecie delineate in materia dal vigente codice sono connotate dal dolo generico e non dal dolo specifico*" (Cass. pen. 26.11.1997, sez. V, n. 1098; Cass. pen. 23.3.2004, sez. V, n. 23324; Cass. pen. 17.2.2004, sez. V, n. 13989, n. 2392; Cass. pen. 30.9.2005, sez. V, n. 35167).

3.2.2 ——— Obbligo di regolare redazione della cartella clinica

Il rapporto che si instaura tra la struttura sanitaria ed il paziente al momento del ricovero è certamente di natura contrattuale e tra gli obblighi strumentali ed accessori, rispetto a quello principale che concerne la prestazione di cure, che gravano sulla struttura vi sono certamente anche quelli che concernono la corretta compilazione della cartella clinica e la sua conservazione, il cui inadempimento è fonte di differenti responsabilità a fini risarcitori per la struttura.
Con riferimento al caso dell'inesatta o incompleta compilazione della cartella clinica, si deve ricordare il recente e costante orientamento sia di legittimità che di merito secondo cui "la possibilità, pur rigorosamente prospettata sotto il profilo scientifico, che la morte della persona ricoverata presso una struttura sanitaria possa essere intervenuta per altre ipotetiche cause patologiche, diverse da quelle diagnosticate ed inadeguatamente trattate, che non sia stato tuttavia possibile accertare neppure dopo il decesso in ragione della difettosa tenuta della cartella clinica o della mancanza di adeguati riscontri diagnostici (anche autoptici), non vale ad escludere la sussistenza di nesso eziologico tra la colposa condotta dei medici in relazione alla patologia accertata e la morte, ove risulti provata la idoneità di tale condotta a provocarla" (Cass. civ. 13.9.2000, sez. III, n. 12103).
Infatti, "la valutazione dell'esattezza della prestazione medica concerne anche la regolare tenuta della cartella clinica: ove dalla sua imperfetta compilazione derivi l'impossibilità di trarre utili elementi di valutazione in ordine all'accertamento della causa (del danno), le conseguenze non possono in via di principio ridondare in danno di chi vanti un diritto" (Trib. Roma 20.1.2004). Nello stesso senso Cass. civ. 21.7.2003, sez. III, n. 11316; Trib. Roma 30.6.2003; Trib. Terni, 3.10.1998, secondo cui "sussiste la responsabilità solidale della Usl e dei medici da essa dipendenti per i danni da questi cagionati al paziente nell'esecuzione dell'attività terapeutica; sussiste, inoltre, la responsabilità diretta della Usl per i danni conseguenti all'erronea compilazione della cartella clinica da parte dei sanitari".
La responsabilità in caso di lacunosa formazione o di mancata conservazione della cartella clinica, si riconnette dunque all'obbligo di controllare la completezza e l'esattezza del suo contenuto, la cui violazione si configura come difetto di diligenza ex art. 1176 comma 2 c.c., da cui consegue la declaratoria di responsabilità della struttura per i danni subiti dal paziente.

Inoltre non si può ritenere che l'incompletezza della cartella clinica possa escludere il nesso di causalità. È infatti giurisprudenza ormai consolidata che in tema di responsabilità professionale del medico la difettosa tenuta della cartella clinica non vale ad escludere la sussistenza del nesso eziologico tra la condotta colposa del sanitario e il danno, ove risulti provata la idoneità di tale condotta a provocare il danno stesso (Cass., 21 luglio 2003, n. 11316).
Si è anzi affermato in giurisprudenza che la sussistenza del nesso eziologico tra la patologia accertata dal medico, verosimilmente idonea a cagionare un pregiudizio al paziente, e il pregiudizio stesso, si deve presumere allorché sia impossibile accertare e valutare altri ipotetici fattori causali proprio in conseguenza della lacunosa compilazione della cartella clinica.
Rispetto agli obblighi di regolare tenuta della cartella clinica è opportuno ricordare, inoltre, che l'art. 26 del Codice di deontologia medica del 2006 prevede che: "la cartella clinica deve essere redatta chiaramente, con puntualità e diligenza, nel rispetto della buona pratica clinica e contenere, oltre a ogni dato obiettivo relativo alla condizione patologica e al suo decorso, le attività diagnostico-terapeutiche praticate" e che il primario è responsabile, ai sensi dell'art. 7 del D.P.R. 27.3.1969, n. 128 "della regolare compilazione della cartella clinica e dei registri nosologici e della loro conservazione fino alla consegna all'archivio centrale".

3.2.3 ——— Trattamento dei dati personali (privacy)

Come detto, nell'ambito del tema della conformità alle normative, riveste un ruolo particolare la conformità a quella sul trattamento dei dati personali. Nell'ambito della CCE, vengono infatti trattati molti di quelli indicati dalla norma come sensibili, e il trattamento di dati sanitari è stato oggetto di norme specifiche.
Il sistema informatico che supporta le funzionalità di CCE deve quindi permettere l'implementazione di specifiche politiche di riservatezza e protezione dei dati, ovvero garantire l'accesso ai dati clinici del singolo paziente esclusivamente agli operatori aventi tale autorizzazione. Da ciò deriva l'esigenza di definire le politiche di gestione dei dati clinici e le conseguenti regole di accessibilità agli stessi in fase di creazione, modifica, cancellazione, lettura. Tali politiche devono essere coerenti con le norme emanate dalle Authority sulla privacy a livello nazionale ed europeo, dalle linee Guida del Ministero della Salute oltre che riflettere eventuali disposizioni regionali. Si precisa inoltre che, per quanto riguarda le tematiche di privacy e fruibilità, i sistemi dovranno prevedere meccanismi alternativi di gestione, applicando le politiche interne definite a livello aziendale.

3.2.3.1 Consenso al trattamento

Preso atto che i sistemi di CCE comportano l'utilizzo di Clinical Datarepository che, a loro volta, costituiscono una parte sostanziale delle architetture di EMR (dossier), riteniamo opportuno richiamare le indicazioni dei Garanti della Comunità Europea in materia di privacy e consenso al trattamento.[7]
Il Documento dei Garanti della Comunità Europea introduce in proposito alcuni requisiti fondamentali in merito al trattamento dei dati sanitari che in parte riconfermano l'impianto complessivo dei contenuti del D. Lgs 196/03 e in parte tendono ad approfondire alcune tematiche. Nello specifico:

- viene riconfermato il **principio di necessità e non eccedenza** dei dati raccolti per uno specifico trattamento e per una specifica finalità (parte seconda, primo capoverso);

[7] Working Document on the processing of personal data relating to health in electronic health records, 00323/07/EN,WP 131, febbraio 2007.

- viene sancito **il rispetto dell'autodeterminazione del cittadino** nella gestione dei propri dati clinici precisando che la "self determination" concerne anche la possibilità di conoscere quando e chi abbia consultato i propri dati clinici (parte terza, primo capoverso);
- viene ribadita la necessità **dell'informativa sul trattamento** e quindi che il cittadino sia reso dettagliatamente informato rispetto all'utilizzo che verrà effettuato dei suoi dati clinici e nel contempo viene precisato che il **consenso** deve essere non solo specifico ma **deve essere riferito a una ben definita e concreta situazione** ("consent must relate to a well-defined, concrete situation") (parte seconda, punto 4), precisando come l'acquisizione del consenso, che deve essere reso in forma esplicita, sia un pre-requisito al trattamento dei dati ai sensi dell'art 8 della Direttiva 95/46/EC. (in tale contesto viene precisato che funzionalità di "approvare" (e quindi disapprovare) nel contesto di opportune misure di salvaguardia è diversa dal "consenso" ai sensi dell'articolo 8 della direttiva e quindi che tale modalità non soddisfa pienamente tutte le prescrizioni dello stesso articolo);
- viene inoltre evidenziato che **l'accesso ai dati sensibili è ammesso solo ai professionisti, autorizzati, che sono coinvolti nel trattamento del paziente**. In particolare si precisa che deve esistere un rapporto di trattamento concreto e attuale tra il paziente e il personale sanitario che desidera accedere ai dati del paziente contenuti nel suo EMR ("There must be a relationship of actual and current treatment between the patient and the healthcare professional wanting access to his EHR record").

In merito alla costituzione del FSE e del Dossier (EMR) il Garante per la protezione dei dati personali ha emesso specifiche linee guida fornendo altresì una prima definizione di "Fascicolo Sanitario elettronico" e "Dossier"; nello specifico si tratta delle "Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario" pubblicate in data 16 luglio 2009 e nella G.U. n. 178 del 3 agosto 2009. Un'altra fonte ministeriale che indirizza la gestione dei dati personali nell'ambito della costituzione del FSE è rappresentata dalle "Linee guida nazionali" in tema di Fascicolo sanitario elettronico redatte dal Ministero della Salute in data 11 Novembre 2010.
Nello specifico il quinto capitolo della pubblicazione illustra i preliminari requisiti di liceità nel trattamento dei dati personali, tra cui riveste particolare importanza l'informativa al paziente e l'acquisizione del suo consenso in applicazione del decreto legislativo del 30 giugno 2003, n. 196 e delle "Linee guida in tema di fascicolo sanitario elettronico (FSE) e dossier sanitario" dell'Autorità Garante per la protezione dei dati personali del 16 luglio 2009.

3.2.3.2 Oscuramento

Nel contesto della CCE per oscuramento dei dati o di un DCE si intende la funzionalità delle applicazioni cliniche che impediscono che i dati del paziente (o una parte di essi) o un DCE siano resi visibili/accessibili/trasmessi a soggetti diversi da quelli che l'hanno prodotto o ad altri programmi applicativi (es. Fascicoli Sanitari Elettronici) e senza che quest'ultimi vengano automaticamente a conoscenza del fatto che l'assistito abbia effettuato tale scelta ("oscuramento dell'oscuramento").
L'oscuramento dei dati (o di una parte di essa) contenuti nella CCE può essere:

- volontario, ovvero richiesto espressamente dal cittadino;
- ex legge ovvero per specifiche disposizioni normative (es. ricoveri IVG);
- nel caso in cui l'oscuramento riguardi l'identificazione del paziente si parla più precisamente di anonimizzazione.

L'"oscuramento" dell'evento clinico è revocabile nel tempo.
I soggetti preposti alla cura possono accedere ai dati del paziente tranne per i casi di oscuramento. I sistemi informativi per la CCE devono gestire le informazioni relative sia alle autorizzazioni fornite dai cittadini sia le regole per l'oscuramento di DCE. In generale il processo di acquisizione della autorizzazione o dell'oscuramento (volontario o ex legge) vengono demandati alla fase di accettazione del paziente all'atto dell'accettazione per prestazioni ambulatoriali o di ricovero. Il sistema di CCE deve quindi essere in grado di acquisire dai sistemi di accettazione tali informazioni per poi gestire queste informazioni in coerenza con le regole che queste riportano (ad es. non trasmissione dei contenute della CCE nel FSE regionale). Parimenti deve gestirne la revoca in tempi successivi.

3.2.3.3 Gestione della Privacy in servizi On-Line

Favorire l'empowerment del paziente è uno degli obiettivi del PSN che può tradursi anche nel rendere disponibili servizi "information intensive". In tale contesto è possibile configurare servizi di prenotazione, pagamento e download di documentazione clinica. Nello specifico, per quanto riguarda la possibilità per il cittadino di accedere al "referto" o altra documentazione clinica in modalità informatica, si evidenzia l'esistenza di regole per la gestione della privacy definite dal Garante della Privacy con proprie specifiche "Linee guida" ufficializzate dopo consultazione pubblica il 19 novembre 2009 e pubblicate sulla G.U. n. 288 dell'11 dicembre 2009.
Le linee guida rendono possibile fornire al cittadino, a sua richiesta, la possibilità di ricevere documentazione clinica via email o via web. In tale contesto le indicazioni contenute nelle linee guida prevedono la necessità di fornire al cittadino un'idonea informativa sulle caratteristiche del servizio di refertazione on-line che può essere resa anche unitamente a quella relativa al trattamento dei dati personali per finalità di cura ma distinta da essa e che preveda l'acquisizione di uno specifico consenso.
Per la ricezione di referti via mail vengono suggerite alcune cautele:

- la spedizione del referto in forma di allegato a un messaggio e-mail e non come testo compreso nella body part del messaggio;
- il file contenente il referto dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati, che potranno consistere in una password per l'apertura del file o in una chiave crittografica rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti (Cfr. regola 24 del Disciplinare tecnico allegato B) al Codice della Privacy;
- la convalida degli indirizzi e-mail tramite apposita procedura di verifica on-line, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall'utente richiedente il servizio.

Anche per il download di documentazione clinica via web, tramite portale di servizi on line, vengono suggerite alcune cautele:

- utilizzo di protocolli di comunicazione sicuri, basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (protocolli https ssl – Secure Socket Layer);

- tecniche idonee ad evitare la possibile acquisizione delle informazioni contenute nel file elettronico nel caso di sua memorizzazione intermedia in sistemi di caching, locali o centralizzati, a seguito della sua consultazione on-line;
- utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di strong authentication;
- disponibilità limitata nel tempo del referto on-line (massimo 30 gg.);
- possibilità da parte dell'utente di sottrarre alla visibilità in modalità on-line o di cancellare dal sistema di consultazione, in modo complessivo o selettivo, i referti che lo riguardano.

3.3 —— Requisiti di sicurezza della CCE

In questa sezione vengono trattati i principali requisiti specifici di sicurezza della CCE.
Abbiamo visto nelle sezioni precedenti che la CCE raccoglie informazioni e documenti disparati e provenienti da fonti diverse, e che tipologie di dati diversi devono essere accessibili a diversi professionisti in modalità diverse, secondo i ruoli assegnati al diverso personale; questi vincoli si sommano alle eventuali ulteriori limitazioni poste dal paziente nell'esercitare i propri diritti sul trattamento dei dati di cui è interessato.
Tutto questo comporta una gestione degli accessi per ruoli sufficientemente flessibile da garantire la tutela della riservatezza in conformità alla normativa. In proposito si richiamano anche le indicazioni del Garante della Privacy in materia di gestione degli accessi degli amministratori di sistema. Appare importante quanto indicato dal Garante: "Devono essere, pertanto, preferite soluzioni che consentano un'organizzazione modulare degli strumenti (NDR di autenticazione e autorizzazione) in modo da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni indispensabili".[8] L'aspetto dell'oscuramento in particolare, è stato già ampiamente trattato nella sezione relativa alla conformità.
Si porrà in generale il problema di garantire la paternità dei dati inseriti in CCE, mediante strumenti (es. firma elettronica) che siano effettivamente accessibili solo a chi ha titolo per utilizzarli.
Per garantire l'integrità dei singoli documenti e delle registrazioni che vengono effettuate sui vari moduli funzionali che compongono la CCE (ad es. attività di nursing, attività di assessment clinico et al.), un ruolo fondamentale riveste la firma elettronica, che garantisce nel contempo l'autenticità del documento e la sua conformità ad alcuni requisiti normativi.
Tuttavia, questo strumento di per sé non è sufficiente a garantire l'integrità della cartella nel suo complesso. L'integrità di una collezione di dati e documenti non è garantita dalla firma di singoli documenti, sia perché non è proponibile di firmare ogni singolo dato, sia perché l'assenza di un intero documento, seppure firmato, non verrebbe rilevata. La tutela dei dati, anche in termini di integrità, deve quindi avvalersi di tutti gli strumenti normalmente utilizzati nell'ambito della sicurezza IT, primo fra tutti l'analisi del rischio che, in funzione di rischi e minacce, porti a misure di sicurezza adeguate.
Si innesta, in tale contesto, il tema delle garanzie generali di correttezza e integrità dei dati.
Per il trattamento cartaceo sono state sviluppate nel tempo procedure ridondate per garantire che errori di trascrizione o altri errori e comportamenti illegittimi o poco accurati comportino rischi per i pazienti.
Sarebbe azzardato supporre che il semplice passaggio ad un trattamento elettronico sia sufficiente per eliminare questi rischi, seppure certamente possa contribuire a ridurli in modo significativo. A titolo esemplificativo, la semplice modifica diretta e manuale di un indice in un database potrebbe avere conseguenze drammatiche, associando dati al paziente sbagliato. Allo stesso modo, un errore nella modifica o nell'aggiornamento dei codici (es. codice riferito ad un trattamento) può avere gravi conseguenze. Si tratta di dati che possono avere origine esternamente alla cartella clinica in senso stretto, e che devono anch'essi essere adeguatamente.
In termini di minacce, si deve qui considerare la "storia" di modifiche effettuate su documenti cartacei, per apprezzare la grande varietà di contesti e motivazioni che hanno nel tempo consentito a livello manuale la produzione di errori o a manomettere i dati in modo da evitare che gli stessi possano essere replicati nel trattamento digitale dei dati.
L'integrità dei dati deve quindi utilizzare dove opportuno dei meccanismi di hash crittografico che siano sufficientemente robusti e che consentano di tracciare i livelli di variazione dei dati.
In questo contesto, particolare rilevanza riveste il tracking degli accessi e delle modifiche: gli strumenti utilizzati dovranno garantire funzionalità adeguate a questa attività come anche alle eventuali attività di audit. Appare opportuno considerare anche strumenti per la rilevazione automatica di anomalie negli accessi da parte di personale autorizzato.
Infine, i dati in transito devono essere protetti in ogni fase della trasmissione e memorizzazione su dispositivi intermedi utilizzati anche da utenti ad esempio per l'accesso online.
Per affrontare correttamente il tema della sicurezza, come detto, deve essere effettuata un'analisi dei rischi. Preso atto che non è possibile affrontare ed esaurire qui una tematica così complessa, si ritiene utile evidenziare alcune indicazioni generali, comprendendo un'analisi delle minacce. Ci limitiamo qui a indicare le minacce tipiche di questo contesto, in modo da poter affrontare i requisiti e le misure di sicurezza nella giusta prospettiva.
Affrontiamo qui il tema secondo i tre aspetti della riservatezza, dell'integrità e della disponibilità.
Si intende comunque che in questo contesto, i requisiti di conformità alle normative sopra esposte saranno considerati come imprescindibili e non affrontati in un'ottica di rischio di non conformità.

[8] "Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario".

3.3.1 —— Riservatezza

La Riservatezza o Confidenzialità si riferisce all'esigenza di tutelare i dati e i servizi contro il rischio di accesso ai dati da parte di soggetti non autorizzati. La tutela della riservatezza richiede fra l'altro l'implementazione di efficaci strumenti di Identity and Access Management (IAM, strumenti di autenticazione e autorizzazione), come anche l'adozione di misure adeguate per la protezione dei dati in transito, sia internamente alla struttura che nelle comunicazioni a soggetti esterni. In particolare la tematica della riservatezza pone l'attenzione almeno su tre criticità:

- la definizione di policy aziendali che definiscano i livelli di autorizzazione al trattamento dei dati, in particolare sensibili;
- il rispetto del principio di necessità nel trattamento dei dati di cui all'art 3 del D. Lgs.196/03 e la cancellazione, dove possibile, di dati eccedenti le finalità del trattamento;

• la cifratura dei database che contengono dati sensibili laddove gli stessi siano associati a dati identificativi.

Oltre a dover tutelare i dati sanitari da accessi da parte di personale non autorizzato, anche l'accesso da parte del personale incaricato può essere oggetto di abusi (ad esempio la curiosità di consultare dati relativi ad amici, parenti o personaggi famosi) e modifiche di dati.

I meccanismi di autenticazione, autorizzazione e controllo accessi possono quindi risultare di per sé insufficienti, perché gli accessi illegittimi possono avvenire anche da parte di chi in generale è autorizzato all'accesso ai dati[9]. Si possono ad esempio considerare strumenti che, pur nell'ambito dei comportamenti autorizzati, possano evidenziare comportamenti anomali, nella stessa logica dei sistemi antifrode.

Non è inoltre da sottovalutare il rischio che errori nelle procedure o negli strumenti espongano i dati anche pubblicamente: a differenza di una cartella cartacea, una CCE accessibile in rete potrebbe per errore divenire accessibile ad un numero imprecisato di soggetti terzi.

L'alterazione di sistemi informatici richiama i contenuti della Legge 547/1993 "modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica". Nello specifico appare interessante segnalare che tale legge modifica il codice penale introducendo in particolare l'art. 635 bis, modificando il 420 e inserendo l'art. 491 bis. L'art. 635 bis adegua il "reato di danneggiamento informatico" ai reati di danneggiamento comune. Una specifica aggravante è prevista dal comma 2 che disciplina il caso in cui il fatto sia commesso "con abuso della qualità di operatore del sistema" (ad esempio alterazioni sw non volute ma effettuate da fornitori in fase manutentiva o da personale formalmente autorizzato ad accedere al sistema); l'art. 420 definisce il sabotaggio informatico come "diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità" inserendo in tale contesto anche "il fatto diretto di danneggiare dati, informazioni o programmi in essi contenuti"; l'art. 491 bis inserisce il reato di falso (materiale e ideologico) ai documenti informatici pubblici e privati estendendo la tutela penale agli strumenti destinati alla elaborazione e produzione di dati nella misura in cui il falso sia stato prodotto da un sistema software appositamente alterato. Si ricorda che per documento informatico a fini penali si intende "qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli" (Iaselli, 2007).

3.3.2 —— Integrità

L'obiettivo dell'**Integrità** è la tutela dall'alterazione di dati, informazioni e/o risorse informatiche. L'integrità comprende quindi differenti tipologie di interventi per evitare la perdita, la modifica (paradossalmente anche la generazione ex novo di dati errati), la cancellazione di dati e informazioni, l'alterazione di sistemi hardware e software, non autorizzata e non voluta.

In tale contesto l'adozione della firma elettronica, nelle sue declinazioni avanzata, qualificata e digitale e del processo di conservazione digitale; integrano il tema dell'integrità affermando i principi di autenticità vale a dire la certezza dell'origine del documento oggetto di firma digitale, di non ripudio inteso come la prevenzione del disconoscimento di un documento da parte dell'autore dello stesso, di opponibilità a terzi attraverso l'apposizione della marcatura temporale che certifica la validità verso terzi di un documento firmato digitalmente.

[9] Vedi ad esempio il caso degli "spioni fiscali" del 2006.

L'integrità dei dati contenuti nella CCE è estremamente critica: errori o modifiche potrebbero comportare rischi gravissimi per i pazienti. In questo contesto, l'integrità si declina in diversi modi:

1. i dati inseriti corrispondano effettivamente al paziente al quale si riferisce la CCE;
2. i singoli documenti inseriti siano effettivamente integri e vengano mantenuti tali;
3. la CCE nel suo complesso sia integra e completa, ovvero che non manchino documenti o dati che ne fanno parte.

Oltre ad eventuali errori nel trattamento e a guasti, vanno considerati due casi importanti:

1. quando il danno derivi dall'accesso a basso livello ai dati, ad esempio nell'ambito delle attività di amministrazione dei sistemi; eventuali errori a questo livello non necessariamente sarebbero rilevabili;
2. quando il danno derivi dalla volontà del personale di modificare o nascondere le informazioni relative a qualche episodio di cosiddetta "malasanità"; questo tipo di abuso sarebbe particolarmente difficile da gestire in quanto compiuto da personale autorizzato al trattamento e quindi abilitato all'accesso.

Un esempio di problema da gestire sarebbe quello in cui una versione della cartella clinica venga sostituita con una versione precedente, in sé integra a tutti gli effetti ma priva ad esempio di un documento. A questo problema si può fare fronte con un "indice della CCE" (previsto ad esempio dalle linee guida della Regione Lombardia) la cui integrità è garanzia di completezza della cartella.

3.3.3 —— Disponibilità

Il tema della disponibilità ha conseguenze importanti dal punto di vista delle architetture e dei sistemi utilizzati per trattare la CCE. Si possono evidenziare alcuni casi importanti dal punto di vista del rischio:

- disponibilità dei dati in presenza di guasti informatici. Si segnala in proposito che l'utilizzo della CCE richiede un'oggettiva attenzione a misure di business continuity sia nelle componenti della server farm sia nella infrastruttura di rete locale e geografica.

  Vanno previste architetture ridondate e di disaster recovery. Si evidenzia anche quanto prescritto dal Garante in merito alla disponbilità dei back-up e del tempo di ripristino dati nel caso di guasti informatici oltre a sottolineare l'importanza di ogni misura atta a evitare la perdita di dati.
- disponibilità dei dati in caso di emergenze mediche; paradossalmente, le misure di sicurezza volte a tutelare la riservatezza dei dati possono costituire il problema principale per questo aspetto, se le procedure autorizzative o di ripristino dei dati sono troppo lente;
- disponibilità dei dati a lungo termine. Tematica fortemente interconnessa alla conservazione sostitutiva del documento "morto".

  In proposito si richiamano i contenuti del nuovo Codice dell'Amministrazione Digitale (Decreto Legislativo 30.12.2010 n.235) che verranno ripresi nei successivi capitoli.
- disponibilità dei dati in occasione di eventi catastrofici, in una logica di business continuity: non solo l'ospedale deve essere in grado di mantenere la propria operatività, per la quale questi dati sono essenziali, ma deve essere anche in grado di fornirli rapidamente ad altre strutture/organismi coinvolti nello stesso contesto di emergenza.

3.3.4 —— Altre misure di sicurezza previste nel vigente quadro normativo in materia di protezione dei dati personali

Le varie misure di sicurezza previste dal D.Lgs. 196/03, noto come Codice Privacy, sono classificate dal legislatore, come anticipato nei precedenti paragrafi, in "**minime**", "**necessarie**" e "**idonee**". In considerazione che la CCE contiene dati idonei a rivelare lo stato di salute dell'interessato/paziente, risulta imprescindibile il rispetto di tutte queste misure di sicurezza.

Nello specifico, le "**misure c.d. minime**", volte cioè ad assicurare un livello minimo di protezione dei dati personali trattati, sono disciplinate dagli artt. 33 e ss. del Codice ed individuate in maniera puntuale dal disciplinare tecnico "Allegato B". In particolare l'art. 34 prevede che:

> "*il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:*
> *a) autenticazione informatica;*
> *b) adozione di procedure di gestione delle credenziali di autenticazione;*
> *c) utilizzazione di un sistema di autorizzazione;*
> *d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;*
> *e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;*
> *f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;*
> *g) … (soppresso);*
> *h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari*".

Le "**misure c.d. necessarie**", invece, vengono di volta in volta individuate dal Garante Privacy - spesso in provvedimenti specifici o Linee Guida emanati ai sensi dell'art. 154, comma 1, lett. c) e d) - nel momento in cui sia necessario regolamentare in maniera puntuale una determinata materia. In tali casi, si prescrive ai Titolari le misure opportune al fine di rendere il trattamento conforme alle disposizioni di legge o si può vietare, in tutto o in parte, un trattamento illecito o non corretto dei dati. Nel caso della CCE si richiama espressamente l'applicabilità di determinate misure di sicurezza elencate nelle Linee Guida emanate dall'Autorità Garante in tema di "FSE e dossier sanitario" e in quelle in materia di "referti on-line".

Le "**misure c.d. idonee**" (disciplinate dall'**art. 31 del Codice**), infine, impongono al Titolare del trattamento dei dati personali la predisposizione di tutte quelle misure di sicurezza idonee a ridurre al minimo "i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta", in modo che i dati personali oggetto di trattamento siano "custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento". Come si può notare, pertanto, i parametri per garantire la sicurezza dei dati personali sono soggetti a continue variazioni dipendenti:

- dalla natura dei dati e dalle specifiche caratteristiche del trattamento (art. 31);
- dalle modalità e le finalità del trattamento;
- dall'ambiente in cui si opera e dei i rischi che corrono i dati;
- dalle conoscenze acquisite in base al progresso tecnologico, fondamentali per garantire il controllo sui dati e la loro custodia.

È opportuno sottolineare, inoltre, che il Codice Privacy prevede, per il trattamento dei dati sensibili e, in particolare per quelli idonei a rivelare lo stato di salute, le seguenti ulteriori misure di sicurezza:

Art. 22, co. 6, Codice Privacy: "I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità".

Art. 92, co. 1, Codice Privacy: Obbligo di adottare opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere quelli relativi al paziente da quelli riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

Sotto un profilo più propriamente giuridico, coscienti delle problematiche sollevate dal trattamento dei dati personali sanitari, già i Garanti europei per la protezione dei dati avevano adottato il 15 febbraio 2007 un documento di lavoro (00323/07/EN WP 131, "Working Document on the processing of personal data relating to health in electronic health records" - EHR), che spiega quali parametri applicativi dovrebbero essere rispettati nell'implementazione e nella gestione dei dati sanitari[10]. Si riportano di seguito alcune indicazioni provenienti dai Garanti Privacy europei e dal Consiglio di Europa:

Cartelle Cliniche Informatizzate - Parere Gruppo Garanti Europei

In tema di cartelle cliniche informatizzate, un parere del Gruppo di lavoro dei Garanti Privacy europei ha stabilito che è necessario:

- dotarsi di una struttura modulare delle cartelle elettroniche per garantire la separazione fra le diverse categorie di dati rispetto alle finalità del trattamento/ai soggetti che vi accedono (Ved. art. 22, comma 7, d.lgs. 196/03);
- prevedere misure di autenticazione, autorizzazione per l'accesso e la comunicazione dei dati;
- adottare sistemi di autenticazione forte e di firma e, quindi, dei veri e propri sistemi di accountability.

Consiglio d'Europa, Raccomandazione R (97) 5)

1. Controllo dell'accesso degli strumenti utilizzati
2. Controllo dei supporti dei dati
3. Controllo delle memorie
4. Controllo delle utilizzazioni
5. Separazione dei dati in:
   - dati identificativi

[10] Nelle Linee Guida dei Garanti UE sono state richieste elevate tutele per i dati sanitari, accessi sicuri e autodeterminazione dei pazienti. Infatti, è stato osservato che la creazione di un sistema nazionale di sanità elettronica è un obiettivo di rilevante interesse pubblico e il relativo trattamento dei dati personali deve avvenire nel pieno rispetto dei principi di protezione a tutela dei dati stessi.

- dati amministrativi
- dati sanitari
- dati sociali
- dati genetici (con controllo dell'accesso)

6. Controllo della comunicazione
7. Controllo a posteriori dell'accesso ai dati
8. Controllo del trasferimento (intercettazione)
9. Controllo della disponibilità (back-up)

Partendo dalle tematiche affrontate in sede europea, la nostra Autorità Garante per la Privacy ha, a sua volta, adottato diversi documenti (quali le Linee Guida in tema di Fascicolo Sanitario Elettronico - FSE - e di Dossier Sanitario - DS - e le più recenti Linee guida in tema di referti on-line o il provvedimento del 26 novembre 2009 in tema di formazione e conservazione delle immagini diagnostiche) con cui ha stabilito i requisiti organizzativi e di sicurezza per trattare in sicurezza i dati sanitari ed essere conformi alle regole previste dalla normativa di settore.
Qui di seguito si riportano alcuni accorgimenti tecnico-normativi per garantire la compliance privacy all'interno di sistemi di gestione della Cartella Clinica Elettronica:

1. Sviluppo di idonei sistemi di autenticazione e di autorizzazione per gli operatori sanitari in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati, sottoscrizione del documento informatico, ecc.).
2. Autenticazione dell'operatore attraverso sistemi di strong authentication: consentire il trattamento dei dati personali, anche di natura sensibile, solo a responsabili o incaricati dotati di credenziali di autenticazione che abbiano superato una procedura di autenticazione (strong authentication) relativa a uno specifico trattamento o a un insieme di trattamenti (ciò consente di fornire le garanzie rispetto all'accesso da parte dei vari operatori specificatamente autorizzati).
3. Adozione di una procedura per la gestione delle credenziali per tutti gli operatori sanitari che possono interagire con il sistema.
4. Qualora una delle componenti l'autenticazione avvenga tramite l'utilizzo di una password, questa deve essere composta da almeno otto caratteri alfanumerici e con le caratteristiche di complessità indicate nell'Allegato B del d. lgs. 196/2003 (modificate dall'utente al primo utilizzo e, a cadenza periodica di almeno tre mesi, imponendo il successivo cambio).
5. Gestire i profili di Autorizzazione, assegnando o associando individualmente a ogni responsabile o incaricato una o più credenziali per l'autenticazione per l'accesso al programma informatico (es. creazione di profili differenziati per l'accesso agli archivi e procedure di autenticazione distinte per i vari profili individuati).
6. Divieto di assegnare il codice per l'identificazione, laddove utilizzato, ad altri incaricati, neppure in tempi diversi.
7. Disattivazione automatica dal sistema informatico delle credenziali di autenticazione non utilizzate da almeno sei mesi, anche nel caso di perdita della qualità che consentiva al responsabile o all'incaricato l'accesso ai dati personali nella CCE.

[11] Tale processo di management dei log deve essere in grado di rappresentare con completezza, per una determinata profondità temporale - che può essere opportunamente commisurata alle esigenze di controllo sul corretto utilizzo della base di dati e degli accessi da parte del titolare del trattamento – l'insieme delle operazioni effettuate sui documenti e deve garantire l'inalterabilità dei log memorizzati. Il periodo di conservazione dei file di log degli accessi e delle operazioni effettuate deve essere ben determinato dal titolare.

8. Utilizzazione di uno specifico e distinto sistema di autorizzazione in base alle informazioni che ciascuno può trattare in funzione dei ruoli e delle esigenze di accesso (quando sono individuati profili di autorizzazione di ambito diverso).
9. Sviluppo di un idoneo sistema di back-up e restore dei dati che garantisca il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
10. Garantire un trattamento disgiunto dei dati idonei a rivelare lo stato di salute contenuti nella CCE dagli altri dati personali che permettono di identificare direttamente gli interessati (separazione logica dei dati idonei a rivelare lo stato di salute dagli altri dati personali trattati per scopi amministrativo-contabili).
11. Cartelle elettroniche con struttura modulare in modo da garantire la separazione fra le diverse categorie di dati rispetto alle finalità del trattamento e ai soggetti che vi accedono.
12. Tracciamento delle operazioni (e loro associazione con l'autore, la data e ora della registrazione): adottare un sistema di tracciabilità degli accessi e delle operazioni effettuate, che consenta un audit ex post degli accessi agli archivi contenenti i documenti sanitari nella CCE per il controllo degli accessi al database e per il rilevamento di eventuali anomalie[11]. Tale sistema deve prevedere anche il rispetto delle misure di sicurezza logiche ed organizzative previste dal provvedimento del Garante per la protezione dei dati personali relativamente alle attribuzioni delle funzioni degli amministratori di sistema.
13. Firma dei contenuti (questa modalità di gestione elettronica rappresenta un miglioramento in termini di tracciabilità, storicizzazione e immodificabilità dei dati rispetto al processo di gestione cartacea del percorso diagnostico, terapeutico e assistenziale).
14. Marcatura temporale e Conservazione.

Al riguardo, è opportuno segnalare come ad oggi siano disponibili molteplici tecnologie ed esistano già molte soluzioni che rispondono alle differenti esigenze di protezione delle informazioni strutturate per:

- proteggere e crittografare i dati sensibili in ambienti di produzione;
- mascherare i dati sensibili negli ambienti non di produzione;
- crittografare il traffico dei dati in rete;
- controllare l'accesso ai dati degli utenti e in particolare degli utenti con privilegi;
- impedire l'accesso da parte degli utenti non autorizzati;
- tenere traccia delle modifiche del database e fare audit delle attività sui dati;
- controllare e bloccare le minacce prima che raggiungano il database.

Per completezza nella trattazione degli aspetti che attengono all'implementazione delle misure di sicurezza privacy in ambito di CCE, è utile richiamare l'applicabilità di alcune prescrizioni emanate dall'Autorità Garante in ambito FSE e referti on-line, oltre che per la conservazione delle immagini diagnostiche e referti che confluiscono nella CCE. È auspicabile, infatti, che il progetto di implementazione della CCE abbia in prospettiva come obiettivo quello di realizzare il dossier sanitario[12] che, come è noto, raccoglie diverse informazioni di carattere sanitario e dati clinici del paziente e poiché si ricade in tale definizione è necessario adottare anche tutte le specifiche misure di sicurezza prescritte dall'Autorità Garante per la protezione dei dati personali nelle sue Linee Guida del 16 luglio 2009.

[12] Potrebbe essere definita anche come una come una "implementazione di dossier sanitario", specificatamente regolamentato dall'Autorità Garante Privacy nelle citate Linee Guida.

Anche in prospettiva di FSE, che prevede la condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e l'intera sua storia clinica, adottare per la CCE le misure di sicurezza previste dal provvedimento del 16 luglio 2009 potrebbe inoltre renderne l'integrazione molto più agevole.

In tema di misure di sicurezza pensate in riferimento alla gestione dei referti on line, invece, è utile richiamare alcune delle prescrizioni specificatamente richiamate per tale tipologia di trattamenti, perché la CCE potrebbe essere messa a disposizione del medico curante del paziente (o di altri professionisti) o resa accessibile (interamente o per determinati documenti) in modalità telematiche, con evidenti problematiche circa la sicurezza e riservatezza dei dati, che in ogni caso il titolare del trattamento dovrà garantire. Un referto, inoltre, di fatto confluisce all'interno della CCE e, se viene creato in modalità digitale, è necessario rispettare tutte le garanzie imposte dalla normativa e dagli specifici provvedimenti del Garante in materia.

Provvedimento del Garante Privacy del 19 novembre 2009: Linee guida in tema di referti on-line

Misure di sicurezza:

Consultazione on line della CCE

- protocolli di comunicazione sicuri, basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (protocolli https ssl - Secure Socket Layer);
- tecniche idonee ad evitare la possibile acquisizione delle informazioni contenute nel file elettronico nel caso di sua memorizzazione intermedia in sistemi di caching, locali o centralizzati, a seguito della sua consultazione on-line;
- utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di strong authentication;
- disponibilità all'utente limitata nel tempo del referto on-line (massimo 45 gg.);
- possibilità da parte dell'utente di sottrarre alla visibilità in modalità on-line o di cancellare dal sistema di consultazione, in modo complessivo o selettivo, i referti che lo riguardano.

Spedizione della CCE tramite posta elettronica[13]

- spedizione della CCE in forma di allegato a un messaggio e-mail e non come testo compreso nella body part del messaggio;
- il file contenente la CCE deve essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati attraverso password per l'apertura del file o in una chiave crittografica rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti (Cfr. regola 24 del Disciplinare tecnico allegato B al Codice)[14].

Ulteriori misure per l'erogazione del servizio on line

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati), prevedendo il ricorso alla strong authentication con utilizzo di caratteristiche biometriche nel caso del trattamento di dati idonei a rivelare l'identità genetica di un individuo;
- separazione fisica o logica dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali trattati per scopi amministrativo-contabili;
- procedure che rendano immediatamente non disponibili per la consultazione on-line o interrompano la procedura di spedizione per posta elettronica a un interessato che abbia comunicato il furto o lo smarrimento delle proprie credenziali di autenticazione all'accesso al sistema di consultazione on-line o altre condizioni di possibile rischio per la riservatezza dei suoi dati;
- adozione di tutte le misure necessarie per rispettare il divieto di diffusione dei dati sanitari (art. 22, comma 8 e 26, comma 5 del Codice Privacy).

Linee guida in tema di Fascicolo sanitario elettronico e di dossier sanitario (FSE)[15]

Linee guida del Garante per la protezione dei dati personali 16 luglio 2009

Misure di sicurezza:

- separazione dei dati a fini amministrativi dai dati sanitari;
- previsione di diversi profili di autorizzazione;
- organizzazione modulare dei dati per limitare il diritto di accesso;
- cifratura file system o database ovvero utilizzo di altri sistemi che rendano inintelligibile il dato;
- idonei sistemi di autenticazione e di autorizzazione in funzione dei ruoli e delle esigenze di accesso e trattamento (in relazione alla possibilità di consultazione, modifica e integrazione dei dati);
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;
- individuazione di criteri per la cifratura o per la separazione dei dati idonei a rilevare lo stato di salute e la vita sessuale dagli altri dati personali;
- tracciabilità degli accessi e delle operazioni effettuate (accountability);
- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie;
- protocolli di comunicazione sicuri con standard crittografici per la comunicazione elettronica tra diversi titolari coinvolti.

3.3.5 —— CCE, integrazione con device elettromedicali, patient safety e sicurezza

La complessità della tematica dei progetti di CCE non può non richiedere un accenno alla problematica dell'integrazione tra CCE e dispositivi medici e introdurre il dibattitto inerente la possibilità o meno che la CCE debba essere intesa come medical device. In proposito appare opportuno evidenziare che la normativa in materia se da un lato lascia ampi spazi di indefinitezza dall'altro è indubbio che solleciti un'attenzione sia alla sicurezza sia alla safety del paziente. In tale contesto si rimanda alle seguenti direttive CE per i dispositivi medici: Direttive 93/42/CEE modificata dalla Direttiva 2007/47/CE recepita con D,Lgs 46/97 e modificata dal

[13] Per l'invio di copia del referto alla casella di posta elettronica dell'interessato, a seguito di sua richiesta.

[14] Tale cautela può non essere osservata qualora l'interessato ne faccia espressa e consapevole richiesta, in quanto l'invio del referto alla casella di posta elettronica indicata dall'interessato non configura un trasferimento di dati sanitari tra diversi titolari del trattamento, bensì una comunicazione di dati tra la struttura sanitaria e l'interessato effettuata su specifica richiesta di quest'ultimo.

[15] In particolare nelle Linee guida per il FSE viene sancito all'art. 3 il "diritto alla costituzione di un Fascicolo sanitario elettronico o di un dossier sanitario" rifacendosi al Codice dell'Amministrazione Digitale (CAD) che, a sua volta, sancisce il diritto dei cittadini all'uso delle tecnologie (art. 3 del CAD).

D.Lgs 37/2010. In tali direttive si evidenzia che per dispositivo medico si intende "qualsiasi strumento, apparecchio, impianto, software, sostanza o altro prodotto, utilizzato da solo o in combinazione, compreso il software destinato dal fabbricante ad essere impiegato specificatamente con finalità diagnostiche e/o terapeutiche e necessario al corretto funzionamento del dispositivo, **destinato dal fabbricante ad essere impiegato sull'uomo** a scopo di diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia".

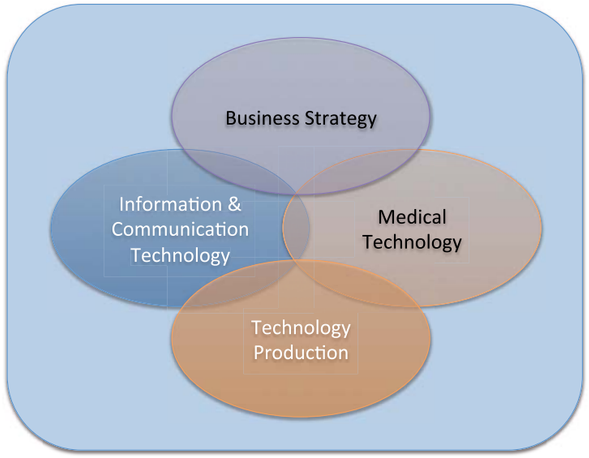
Appare indubbio, in tali direttive e nei D.Lgs attuativi, il richiamo al "software" ma se ne evidenzia un utilizzo diretto "**sull'uomo**" lasciando oggettivi spazi interpretativi in quanto la CCE non utilizza sw direttamente connessi all'uomo.

Non è ovviamente questa la sede per la definizione o meno della CCE come sw medicale e quindi sulla necessità o meno che lo stesso sia oggetto di "analisi del rischio e certificazione" secondo Direttiva sui DM (2007/47/CE). Si segnala l'opportunità che tale argomento coinvolga oltre al mondo professionale (sistemi informativi e ingegneria clinica) anche il mondo della ricerca scientifica, della produzione e gli organismi istituzionali con l'obiettivo di ipotizzare soluzioni "sostenibili".

In tale contesto si segnala che il problema principale, nell'operatività quotidiana, non deriva da una eventuale certificazione della CCE come dispositivo medicale ma dalla concreta possibilità di connettere alla rete aziendale i dispositivi medicali e di integrare tali dispositivi al sistema informativo aziendale e alla CCE prendendo atto che le direttive sopra richiamate obbligano il fornitore a "corredare il dispositivo delle informazioni per garantirne un'utilizzazione sicura" e di conseguenza vincolano le Aziende Sanitarie ad "**usare il dispositivo medico esattamente come indicato dal fabbricante**".

Articoli apparsi anche recentemente sulla stampa nazionale e riferiti a ricerche effettuate dal National Institute of Standards and Technology statunitense evidenziano in proposito che con una certa frequenza i sistemi operativi installati sui dispositivi medici non sono aggiornati, spesso non consentono l'installazione di antivirus o altri requisiti di sicurezza normalmente previsti per i sistemi informatici che compongono il sistema infrormativo aziendale determinando due tipologie di problemi: un primo problema riconducibile alla patient safety in quanto è stato dimostrato che è possibile introdursi nel sistema operativo di sicurezza: attraverso bugs di sistema è possibile introdursi nel sw operativo del sistema medicale e determinare modifiche nel funzionamento degli stessi (ad es. è stato dimostrato che, con l'uso di un un computer portatile, è possibile inviare a distanza una serie di shock con una potenza di 830-volt ai peacemaker); un secondo problema determinato dalla possibile propagazione di infezioni virali attraverso la rete aziendale dato che, con una certa frequenza, i dispositivi medici non possono essere gestiti con le policy di sicurezza normalmente utilizzate per la restante tecnologica connessa alla rete aziendale.

Ancora una volta, considerando i rischi connessi alla safety e alla security, pur evidenziando che la prima ha un'indubbia rilevanza per le possibili complicanze sulla salute del paziente, si suggerisce la massima cautela in fase di implementazione evidenziando che questa tematica deve essere trattata in modo multidisciplinare, coinvolgendo quindi informatici, clinici, ingegneri clinici, produttori al fine di attivare tutte le azioni possibili per ridurre i rischi connessi all'utilizzo di tali tecnologie integrate al sistema di CCE e, di conseguenza, all'intero sistema informativo aziendale in un'ottica di utilizzo di tecnologie diverse al fine del raggiungimento degli obiettivi strategici e di politica sanitaria definiti dalle direzioni aziendali.



3.4 —— Sistema di autenticazione e autorizzazione della cartella clinica elettronica, Sign On, gestione dei log e business continuity

3.4.1 —— Sistema di autenticazione e autorizzazione

L'utilizzo della CCE basata su un Clinical Data Repository che, come abbiamo visto consente una ricomposizione longitudinale nel tempo, di tutte le informazioni clinico-assistenziali di un cittadino, richiede che tali informazioni siano fruibili solo al cittadino (o alle persone da lui autorizzate) e ai team medico-infermieristici che sono coinvolti nel processo di cura dello stesso.

Ne consegue che l'avvio di progetti di CCE richiede specifiche attenzioni alle problematiche legate all'autenticazione e all'autorizzazione. Le considerazioni di seguito riportate fanno riferimento alla CCE ma in generale possono essere applicate all'intero sistema informativo dell'azienda sanitaria. Infatti il Sistema Informativo dell'azienda è costituito da un vasto insieme di risorse (funzionalità applicative, dati, documenti) che devono poter essere accedute solo da soggetti riconosciuti ed autorizzati.

Qualora l'azienda sia dotata per l'intero sistema informativo di:

- un sistema di autenticazione ovvero un sistema centralizzato volto ad accertare l'identità degli utenti che accedono al sistema;
- un sistema di autorizzazione ovvero un sistema centralizzato in grado di garantire che solo gli utenti aventi le abilitazioni necessarie possano utilizzare una specifica funzione o dati disponibili nel sistema.

Occorre verificare che la cartella clinica sia capace di interfacciarsi con i sistemi di cui sopra in base agli standard e specifiche già previste dall'azienda per i suddetti sistemi.

Qualora così non fosse il software della CCE deve prevedere servizi di sicurezza applicativa in grado di:

- identificare i soggetti che accedono ad una risorsa (servizio di Autenticazione): il soggetto che richiede di accedere ad una risorsa della CCE deve farsi riconoscere tramite la presentazione di opportune credenziali; a seguito dell'identificazione dell'utente, viene generata una "identità digitale", cioè una rappresentazione della persona fisica nel software della cartella clinica;

- autorizzare il soggetto ad accedere ad una risorsa (servizio di Autorizzazione): sulla base della risorsa richiesta, dell'identità digitale del soggetto, del ruolo del soggetto e delle politiche di autorizzazione definite, il servizio di Autorizzazione decide se concedere o meno l'accesso a una o più funzioni della CCE.

Esistono diversi tipi di credenziali di autenticazione, che si differenziano per:

- il grado di imputabilità, cioè la forza dell'associazione della credenziale alla persona fisica che la presenta; è una caratteristica che deriva dalla modalità con cui viene consegnata la credenziale al soggetto, cioè dal processo che viene definito per la registrazione di un utente all'interno di una comunità (ad esempio: una credenziale di tipo "username + password" consegnata alla persona dopo il suo riconoscimento de visu è più forte della stessa credenziale scelta da un utente in una procedura online);
- il grado di sicurezza del dispositivo: è la caratteristica intrinseca del dispositivo che ospita la credenziale. Ad esempio, una chiave privata generata e conservata nel chip crittografico di un dispositivo (ad esempio smart card, chiavetta USB, dispositivo OTP) è una credenziale intrinsecamente più sicura di una chiave generata e conservata su un PC, in quanto la smart card o un dispositivo OTP è uno strumento che il titolare può sempre portare con sé, ogni operazione crittografica viene eseguita su di essa e non sul PC ospite e nel suo utilizzo è sempre protetta da un PIN;
- la tipologia della credenziale di autenticazione: è una classificazione relativa alla natura della credenziale.

Le credenziali vengono usate dal servizio di autenticazione per identificare gli utenti mentre l'identità digitale viene utilizzata dal servizio di autorizzazione per verificare il diritto di accesso alle varie funzioni del Sistema Informativo o della CCE in base al ruolo definito per l'utente. Allo scopo di garantire l'integrità e il non-ripudio dei dati/documenti che vengono generati e scambiati dagli operatori sanitari nell'ambito delle loro attività e al contempo la loro autenticazione, si suggerisce di rilasciare un dispositivo crittografico dotato di:

- un certificato digitale di autenticazione - utilizzato dalle procedure di autenticazione per identificare il titolare del dispositivo;
- un certificato di firma digitale - utilizzato per apporre la firma elettronica qualificata (firma digitale) a documenti informatici.

L'adozione di un dispositivo crittografico consente in sostanza di poter garantire l'"autenticazione forte" basata sulla cosiddetta two-factor authentication: "qualcosa che l'utente conosce" (ad es. una password o un pin) + "qualcosa che l'utente possiede" (ad es. un dispositivo per la generazione di un token di autenticazione di tipo One Time Password – OTP, o un certificato digitale associato all'identità dell'utente).

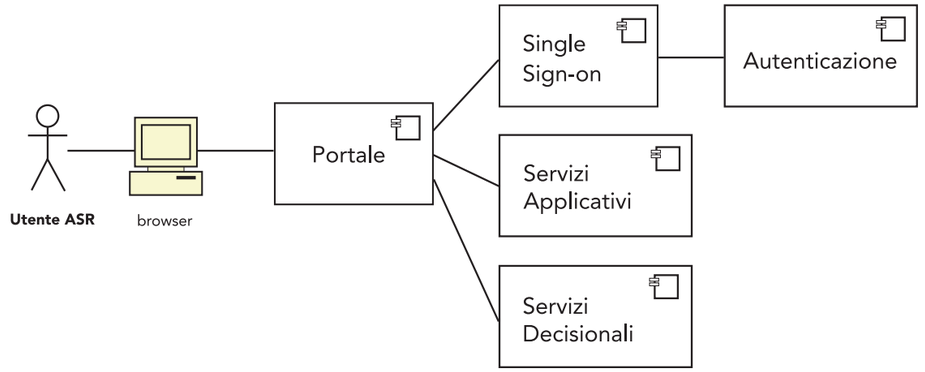
Pertanto il rilascio di un dispositivo crittografico implica che sia definito un processo per:

- il provisioning delle credenziali;
- il servizio di gestione dei dispositivi e delle credenziali crittografiche per monitorare gli eventi in scadenza e le fasi di rinnovo, in modo che non ci siano interruzioni nell'operatività dell'azienda.

3.4.2 —— Single Sign-On (SSO)

Per ottimizzare e rendere più efficace e pratica l'autenticazione dell'utente è opportuno prevedere un meccanismo di Single Sign-On (SSO) che permetta agli utenti di autenticarsi una sola volta e di accedere poi liberamente a tutte le risorse informatiche alle quali sono abilitati, senza dover digitare password diverse per ogni applicativo in uso. La componente di SSO si appoggia al sistema di autenticazione centralizzato che dovrebbe essere integrato con l'anagrafe degli operatori, tendenzialmente alimentata dal sistema HR (Human Resource) dell'azienda sanitaria e basata su un sistema Ldap.

A tale proposito si ricorda che la presenza di un portale, in ambito Intranet o Internet, consente agli utenti di avere un punto di ingresso univoco all'insieme delle applicazioni software disponibili. Proprio in quanto fornisce una vista unificata sui servizi applicativi, è importante che il portale sia integrato con il meccanismo di Single Sign-On (SSO) in modo da realizzare una gestione centralizzata dell'autenticazione degli utenti (vedi schema sottoriportato).



Sulla base di quanto sopra affermato, si suggerisce, di verificare che il software della cartella clinica sia basato su soluzioni tecnologiche integrabili all'interno di un portale, in modo tale da ridurre al minimo le modifiche e gli adattamenti richiesti per una sua fruizione.

3.4.3 Sistemi di autenticazione federati o centralizzati

Nell'ambito dell'accesso alla CCE si deve considerare anche la necessità che soggetti esterni all'ospedale possano accedere ai dati. L'ospedale non è infatti un'entità isolata, ma si colloca all'interno di un sistema sanitario regionale e nazionale che prevede ad esempio che medici della stessa regione possano accedere alla CCE nell'ambito più complessivo del FSE, in cui i dati siano comunque conservati dalle singole strutture che ne sono Titolari e che quindi li devono rendere accessibili a soggetti esterni.

Sarà necessario quindi disporre di meccanismi di autenticazione e autorizzazione che consentano di integrare soggetti non definiti internamente alla struttura, per il solo accesso ad alcune funzioni della CCE. Questo può essere ottenuto con un'integrazione con i sistemi di altre strutture, tipicamente regionali. Questa integrazione può avvenire sia mediante sistemi federati che mediante la centralizzazione della gestione di questi accessi applicativi esterni presso un'unica struttura, ad esempio a livello regionale.

3.4.4 Gestione dei log

Le attività di tracciatura su file di log del software di Cartella Clinica per finalità di sicurezza, e non solo, sono determinate, come già evidenziato, dall'esigenza di registrare le operazioni effettuate da qualsiasi utente autorizzato al suo utilizzo con l'obiettivo di ricostruire gli eventi e le conseguenti responsabilità sui trattamenti di dati personali/sensibili (responsabilità medico-legali).

È necessario quindi, quale misura cautelare, registrare e mantenere la registrazione delle attività svolte dalle varie entità quali la scrittura, la lettura, l'aggiornamento e la cancellazione dei dati trattati, determinando una sorta di "journaling" che consenta di risalire con certezza all'autore di una determinata operazione.

Le caratteristiche di sicurezza di tali registrazioni, devono quanto meno rifarsi ai requisiti di completezza, inalterabilità e possibilità di verifica dell'integrità, già richiamate dal Garante in materia di protezione dei dati personali nel Provvedimento del 27 novembre 2008 riferito agli "Amministratori di Sistema" (G.U. n. 300 del 24 dicembre 2008), ma prevedere ovviamente tutte le altre misure di sicurezza idonee discusse nei precedenti paragrafi.

In riferimento ai log generati in conformità al Provvedimento sugli Amministratori di Sistema sopra citato, questi rappresentano, per finalità e contenuto, altra tipologia di log. Le informazioni rilevabili in tali log si deducono dalle disposizioni contenute nell'art. 2, lett. f, del citato provvedimento del Garante che espressamente recita: "Registrazione degli accessi - Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi".

Come si può dedurre, le informazioni contenute in tali log, oltre a riferirsi alle sole figure degli Amministratori di Sistema, non contengono elementi necessari per tutelare i possibili abusi del sistema di sicurezza dell'infrastruttura IT in un ambiente sanitario, in quanto occorrerebbe integrare tali log con vere e proprie soluzioni di "Change Management" e "Security Management".

Questi log prodotti per le finalità di monitoraggio e controllo del sistema non dovrebbero contenere dati personali, riservati, sensibili o giudiziari.

3.4.5 Piano di Business Continuity e di Disaster Recovery

Parlando di sicurezza dei dati, ed in particolar modo di quelli di carattere sanitario, un elemento cardine è la continua **disponibilità** degli stessi. In altre parole il piano di sicurezza deve necessariamente tener conto anche della continuità del servizio per garantire la disponibilità delle informazioni cliniche.

Inutile sottolineare le conseguenze della indisponibilità di una informazione sanitaria in caso di impellente necessità di accedere a tali informazioni per decisioni da prendere a tutela della salute dell'interessato.

Più in generale quello che occorre prevenire e poter gestire è una "situazione di crisi" che le strutture sanitarie, pubbliche o private che siano, devono necessariamente attrezzarsi ad affrontare, puntando a diventare una organizzazione "resiliente", cioè in grado di acquisire la capacità di cambiare ed adattarsi prima che una situazione di rischio le costringa a farlo (principio di flessibilità). Questo significa che il punto di partenza non è la tecnologia ma "l'Executive management", cioè quel "Comitato di gestione della crisi" (CGC) che dovrebbe essere costituito per gestire e affrontare situazioni di crisi, composto da soggetti che hanno il potere (Top Management) di prendere decisioni finalizzate a proteggere le persone (quindi la salute), i beni materiali e immateriali, la continuità operativa e, quindi, la reputazione dell'azienda.

Le linee guida redatte da DigitPA per la continuità operativa ed il disaster recovery delle Pubbliche Amministrazioni, infatti, individuano i componenti del "Comitato di gestione della crisi" in:

- un ruolo di vertice con poteri decisionali e di indirizzo in materia organizzativa ed economica, ovvero il responsabile dell'Ufficio Dirigenziale ex art. 17 del CAD;
- il Responsabile della "continuità operativa" dell'Ente;
- il Responsabile dell'Unità locale di sicurezza prevista dal DPCM 01.04.2008;
- i referenti tecnici (anche fornitori di servizi ICT) di volta in volta necessari alla gestione della crisi;
- il responsabile della logistica;
- il responsabile della safety dell'ente.

In realtà andrebbe definito un vero e proprio piano di crisi che oltre a determinare i componenti del CGC individui le loro figure di backup (persone alternative), le modalità per contattarli (7/24), un leader del CGC con almeno due back-up, un metodo di comunicazione per attivare il CGC e per disattivare lo stato di crisi, oltre ad una chiara definizione dei criteri di ingaggio/invocazione del CGC. Il CGC dovrebbe avere dei compiti molto precisi e ben individuati ed assegnati ai suoi membri. È importante che definisca strumenti operativi chiari e disponibili in caso di emergenza in modo che ognuno sappia chiaramente cosa fare per reagire ad uno stato improvviso di crisi (Wallet Card, Calling Tree, punti di invocazione, ecc) e definisca politiche, come ad esempio la cosiddetta "Clear desk policy" che oltre a migliorare la produttività, è essenziale per la protezione dei dati sensibili.

Le citate Linee Guida di DigitPA, oltre a definire la periodicità con la quale il CGC deve riunirsi e le aree che devono supportarlo (logistica, tecnologica, informazioni, comunicazioni, finanza, risorse umane, sicurezza informatica, legale), prevedono i seguenti compiti del CGC:

- definizione ed approvazione del piano di continuità operativa;
- valutazione delle situazioni di emergenza e dichiarazione dello stato di crisi;
- avvio delle attività di recupero e controllo del loro svolgimento;
- rapporti con l'esterno e comunicazione ai dipendenti;
- attivazione del processo di rientro che deve essere attuato dagli specifici gruppi operativi, ma deve essere continuamente monitorato dal Comitato, per assicurare la verifica dello stato di avanzamento complessivo e risolverei casi dubbi, omissis…;
- avvio delle attività di rientro alle condizioni normali e controllo del loro svolgimento;
- dichiarazione di rientro;
- gestione di tutte le situazioni non contemplate;
- gestione dei rapporti interni e risoluzione dei conflitti di competenza;
- promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità.

Nelle stesse linee guida, inoltre, si fa riferimento ad un cosiddetto "Gruppo di supporto" al CGC, costituito essenzialmente da tecnici, cui poter delegare il compito di:

- redazione del piano di continuità operativa e proposta al CGC per l'approvazione;
- gestione e manutenzione del piano di continuità operativa;
- adeguamento periodico dell'analisi di impatto (BIA);
- studio di scenari di emergenza e definizione delle strategie di rientro;
- gestione dei rapporti con le assicurazioni;
- attuazione delle attività di divulgazione e di sensibilizzazione interna sui temi della continuità.

Non bisogna però dimenticare che la Business Continuity (o Continuità Operativa) è da sempre materia di manager e non di tecnici e che se ben gestita ha un importante ritorno in termini di miglioramento dei processi gestiti. La BC, infatti, ha successo solo attraverso un approccio Top-bottom (il Top Management impone la BC) e se ben incastonata nella cultura dell'azienda sanitaria, deve essere definita secondo i seguenti passaggi:

- esecuzione di una BIA (Business Impact Analisys) per ogni processo critico (dichiarati dal Top Management);
- selezione dei processi critici da inserire in BC;
- definizione del Piano di BC per ogni processo selezionato (o inserimento nel Piano di BC generale dei processi selezionati).

La BIA è uno strumento fondamentale per la gestione dei rischi - da non confondere però con la loro valutazione - utilizzato per misurare l'impatto negativo causato dalla perdita o alterazione di un processo aziendale i cui risultati servono per decidere le strategie da adottare per mitigare i rischi stessi e supportare le risorse e i servizi da condividere nelle fasi di emergenza. Ha come obiettivi, tra gli altri, quello di fornire un fondamento logico a un piano di BC, identificare i processi e gli asset che richiedono il più alto livello di protezione, rilevare e rivelare i Singol Point of Failure, fornire informazioni utili all'identificazione di strategie alternative, stabilire Recovery Objectives e scadenze.

Un Piano di BC deve a sua volta definire:

- CHI ha la responsabilità delle azioni di recupero;
- COSA è necessario per recuperare o continuare l'operatività;
- DOVE continuare le funzione e la continuità;
- QUANDO devono essere ripristinate le funzioni e l'operatività;
- COME effettuarne il recupero.

Le chiavi di successo di un piano di BC risiedono nella sua chiarezza, flessibilità, essenzialità e allo stesso tempo completezza con check list dei vari task, inclusione delle risorse chiave e delle loro alternative, costantemente aggiornato e formulato sul "Worst case scenario".

Elemento importante della BC è il piano di Disaster Recovery, il cui sviluppo deve generalmente seguire un percorso articolato nelle seguenti fasi:

1 - Classificazione dei processi critici (ereditata dalla BC).

2 - Definizione dei criteri e dei parametri del piano.

3 - Determinazione di tutte le applicazioni da includere nel piano.

4 - Definizione dei requisiti del piano di Disaster Recovery.

Da questa fase ci si attende la definizione dei punti sotto indicati:

- modalità ed entità di utilizzo dei sistemi nella fase di Disaster Recovery, sia a livello di impegno di risorse elaborative e di gestione delle stesse, sia a livello utente;
- architetture di sistema e di rete alternative;
- fonti e soluzioni per il reperimento e la disponibilità di sistemi e reti alternative;
- eventuali polizze assicurative;
- interfacce, interscambi e/o interconnessioni tra i vari sistemi di procedure;
- verifica delle procedure di back-up per le applicazioni incluse nel piano;
- definizione della struttura organizzativa di gestione della crisi.

5 - Progettazione di dettaglio del piano. Questa fase consiste nella definizione, a livello dettagliato, delle procedure e delle regole comportamentali da seguire, da parte del personale coinvolto, sia in fase di gestione corrente che al momento della dichiarazione della crisi e, conseguentemente, di attuazione del piano.

6 - Implementazione del piano. In questa fase si procede alla redazione finale delle procedure, al consolidamento dell'organizzazione necessaria per attuarle, all'acquisizione delle risorse software, hardware e logistiche necessarie.

7 - Test pre-operativo. Questa fase consiste nell'effettuazione del collaudo dell'intero piano, prima del rilascio a livello operativo, e della relativa attività di formazione.

8 - Test operativi periodici e aggiornamento. La fase si concretizza nell'effettuazione di esercitazioni periodiche di attivazione parziale e/o totale del piano, nonché nella definizione e messa in pratica dei criteri per la manutenzione ordinaria e straordinaria dello stesso.

Si ritiene opportuno, infine, ricordare che l'art. 50-bis del CAD ha introdotto per le Pubbliche Amministrazioni, diversi obblighi, tra i quali, si evidenzia in particolare quelli di cui al comma 3 che testualmente prevede:

"A tali fini, le pubbliche amministrazioni definiscono:

a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la Pubblica Amministrazione e l'Innovazione".

È da sottolineare l'importanza e il lavoro, andato forse anche ben oltre il mandato ricevuto, svolto da DigitPA nella redazione delle linee guida per le PA, che rappresentano un'utile guida per affrontare un progetto di Business Continuity con riferimenti a norme, standard ISO ed istruzioni chiarificatrici, richiamate spesso nel presente documento, ove è consigliabile e opportuno fare riferimento per una trattazione più approfondita di taluni aspetti, oltre che alle fonti da queste linee guida richiamate, quali ad esempio quanto prodotto dal Business Continuity Institute, ai quali si rimanda per una esaustiva trattazione di questi temi.

3.5 ——— Valore documentale della CCE: redazione, conservazione, esibizione

3.5.1 ——— La rilevanza probatoria della cartella clinica nel processo civile

Oltre agli obblighi di regolare redazione sopra evidenziati, è opportuno sottolineare, per gli aspetti che qui interessano, che la cartella clinica rappresenta, altresì, un elemento centrale e fondamentale nel quadro probatorio che le parti offrono al giudice civile per risolvere le eventuali controversie in merito a questioni attinenti alla responsabilità medica.

Anche se parte della dottrina e della giurisprudenza di legittimità delle sezioni civili della Cassazione, non condivide la posizione assunta dalle sezioni penali del Supremo Collegio sopra ricordate ed assegna alla cartella clinica la natura di certificazione amministrativa[16], si può affermare che l'efficacia probatoria della CCE, intesa quale documento informatico all'interno del quale potranno confluire le informazioni relative ai dati sanitari e alla storia clinica del paziente, è essenziale dal punto di vista anche del giudizio che il paziente o i suoi parenti potrebbero intentare nei confronti dei professionisti sanitari e della struttura sanitaria a cui appartengono.

Da quando la giurisprudenza ha riconosciuto come "fondamentale" il diritto del paziente di esprimere il consenso informato rispetto al trattamento medico è stato, infatti, avvertito in modo ancora più evidente il problema della sua corretta e idonea documentazione.

Le registrazioni effettuate in cartella clinica dai vari professionisti sanitari coinvolti nel processo di cura del paziente assumono, pertanto, un particolare rilievo quali informazioni incorporate in un documento che deve rispondere necessariamente a requisiti formali suscettibili di attestarne l'autenticità, l'integrità e la completezza[17].

In una simile prospettiva diventa particolarmente apprezzabile - come è stato recentemente più volte evidenziato[18] - l'efficacia probatoria in giudizio della CCE, intesa come documento informatico, in quanto maggiormente idonea a garantire e conservare l'autenticità e l'integrità del contenuto rispetto ad eventuali manipolazioni da parte di terzi.

Ciò naturalmente qualora siano rispettate tutte la caratteristiche di affidabilità, sicurezza, integrità e immodificabilità che un documento informatico può avere solo se formato e conservato nel rispetto di quanto previsto dal D.lgs. 7 marzo 2005, n. 82 e successive modifiche e integrazioni.

3.5.2 ——— Valore legale ed efficacia probatoria della CCE

Dall'analisi della dottrina e della giurisprudenza sul valore documentale e sulla funzione svolta dalla cartella clinica in campo medico-legale, emerge con assoluta chiarezza che il progetto di implementazione della CCE, intesa come documento informatico valido legalmente e con efficacia probatoria - e, quindi, sostitutiva della cartella clinica cartacea - deve necessariamente assicurare non solo la tracciabilità di tutte le registrazioni informatiche effettuate in ogni fase del processo diagnostico-terapeutico-assistenziale, ovvero consentire di risalire a chi e quando ha effettuato ogni singola registrazione, ma anche garantire l'autenticità, l'integrità e l'immodificabilità dei documenti che vi afferiscono.

Questi particolari requisiti della CCE possono essere soddisfatti solo attraverso un adeguato utilizzo della firma elettronica che, come è noto, costituisce un supporto sia per garantire la tracciabilità in fase di inserimento e modifica di dati clinici sia per garantire l'integrità di documenti clinici prodotti con sistemi di CCE o sistemi ad essa correlati.

Il diverso valore probatorio e la diversa usabilità delle varie soluzioni di firma tecnicamente realizzabili e previste dalla vigente normativa, richiedono però alcuni chiarimenti iniziali prima di valutare la loro effettiva utilizzazione in una soluzione di CCE.

La firma digitale, ad esempio, pur essendo il sistema di firma elettronica che attualmente fornisce maggiori garanzie giuridico-probatorie, presenta ancora difficoltà di utilizzo dovute, in gran parte, ad una scarsa conoscenza da parte del firmatario delle corrette modalità di utilizzo dello strumento di firma, ma anche ad una normativa che, ancora oggi, lascia qualche zona d'ombra. Anche per questo motivo, accanto alla firma digitale, occorre riflettere sull'utilizzabilità di processi di sottoscrizione meno rigidi che possano comunque rientrare nell'alveo delle firme elettroniche avanzate (FEA).

3.5.3 ——— Le diverse tipologie di firme elettroniche e loro valore probatorio

Il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) così come modificato dal D.Lgs. 235/ 2010, prevede le seguenti quattro diverse tipologie di firme elettroniche:

- **firma elettronica**: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
- **firma elettronica avanzata**: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
- **firma elettronica qualificata**: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
- **firma digitale**: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Se il comma 1 dell'art. 21 del CAD prevede che "*Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio*[19]*, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità*", il successivo comma 2 continua affermando che "*il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del Codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria*".

La normativa primaria, quindi, mentre riconosce ai documenti sottoscritti con firme elettroniche "*semplici*" un

[16] Su questo aspetto la giurisprudenza civilistica si è espressa nel senso che "le attestazioni contenute in una cartella clinica sono riferibili ad una certificazione amministrativa per quanto attiene alle attività espletate nel corso di una terapia o di un intervento, mentre le valutazioni, le diagnosi o comunque le manifestazioni di scienza o di opinione in essa contenute non hanno alcun valore probatorio privilegiato rispetto ad altri elementi di prova; in ogni caso, le attestazioni della cartella clinica, ancorchè riguardante fatti avvenuti alla presenza di un pubblico ufficiale o da lui stesso compiuti (e non la valutazione dei suddetti fatti) non costituisce prova piena a favore di chi le ha redatte, in base al principio secondo il quale nessuno può precostituire prova a favore di se stesso". (Cass. civ. 27.9.1999, sez. III, n. 10695; Cass. Civ. 12.5.2003, sez. III, n. 7201).

[17] Interessanti a questo proposito risultano essere le osservazioni contenute in U. Izzo, "Medicina e diritto nell'era digitale: i problemi giuridici della cyber medicina", in "Danno e resp., 2000, 8/9, 807 ss." e in particolare quella che evidenzia che sempre di più si assiste ad una sorta di "eterogenesi dei fini": l'informazione fornita per curare è, al contempo, un dato per giudicare.

[18] Si veda a questo proposito Camilla Filauro, "Telemedicina, cartella clinica elettronica e tutela della privacy", in "Danno e responsabilità 5/2011.

[19] Vale a dire che in sede giudiziaria l'efficacia probatoria della firma elettronica "semplice" sarà nei fatti una diretta conseguenza dei processi tecnologici e organizzativi posti in essere.

valore giuridico e probatorio assodato ma difficilmente valutabile a priori, riconosce ai documenti sottoscritti con firme elettroniche avanzate (e in questa macro categoria rientrano anche le firme digitali e le altre firme qualificate) un valore probatorio ben preciso, ovvero quello riconosciuto alle scritture private che, secondo quanto previsto dall'art. 2702 del nostro Codice civile, fanno piena prova, fino a querela di falso, della provenienza delle dichiarazioni di chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.
La sottoscrizione, quindi, di un documento elettronico con una firma elettronica avanzata equivale pienamente alla sottoscrizione "analogica" su carta. L'unica eccezione è contenuta nel comma 2-bis dell'art. 21 del CAD, secondo il quale "*le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del Codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale*".

3.5.3.1 ——— La firma digitale

Per comprendere come, in concreto, funzioni la firma digitale, bisogna innanzitutto tener presente che essa si basa su un **cifrario asimmetrico**: è, dunque, fondata sull'uso di due chiavi diverse, generate insieme nel corso di un unico procedimento. Una delle due chiavi serve per cifrare (**chiave diretta**), l'altra per decifrare (**chiave inversa**).
Le proprietà fondamentali di un tale sistema sono:
- non si può decifrare il testo con la stessa chiave usata per cifrarlo;
- le due chiavi sono generate con la stessa procedura e correlate univocamente;
- conoscendo una delle due chiavi, non c'è nessun modo di ricostruire l'altra.

In tal modo, una delle due chiavi può essere resa pubblica, mentre l'altra deve essere mantenuta segreta.
A questo punto, il sistema più elementare per garantire al terzo la provenienza e l'integrità del documento sarebbe quello di inviargli un testo chiaro insieme ad una versione dello stesso cifrata con la chiave privata del mittente. Il destinatario sarebbe chiamato a decifrare il testo con la chiave pubblica del mittente e, se i due testi risultassero uguali, otterrebbe entrambe le certezze sull'identità del mittente e sull'integrità del contenuto.
Tuttavia, un sistema del genere è lento, perché bisognerebbe cifrare e decifrare tutto il documento, operazione che può richiedere molto tempo anche perché è strettamente connessa alle capacità dell'elaboratore utilizzato. Per ovviare ad un simile inconveniente si ricorre allora a una semplificazione che consiste nel cifrare solo un brevissimo riassunto del testo stesso, ottenuto con una procedura detta funzione di **hash**: tale funzione restituisce pochi caratteri che costituiscono l'impronta del testo (**digest**).
Se alla fine della procedura l'impronta che risulta dalla decifratura con la chiave pubblica del mittente è uguale a quella che si ottiene applicando la funzione di hash al testo chiaro, vuol dire che esso proviene da chi appare come il titolare della chiave pubblica e che non è stato alterato dopo la generazione della firma digitale.
Quanto delineato ruota attorno a un perno centrale che è quello della **conoscibilità della chiave pubblica**, con il corollario della sua attendibilità.

Se la comunicazione deve svolgersi tra due soggetti che si conoscono, essi possono direttamente scambiarsi le rispettive chiavi pubbliche. Ma il grande vantaggio dei sistemi di crittografia a chiave asimmetrica è proprio la possibilità di rendere pubblica una delle due chiavi, consentendo a chiunque di controllare che un messaggio provenga proprio dal titolare dell'altra chiave - quella privata - e che non sia stato alterato o contraffatto.
Naturalmente, la pubblicazione e il controllo delle chiavi si svolgono per via telematica, accedendo ad appositi registri, che costituiscono il punto critico del sistema.
Infatti, è indispensabile che i gestori di questi registri siano soggetti assolutamente scrupolosi e fidati e che siano, in qualche modo, a loro volta, certificati. Sarebbe, altrimenti, assai agevole per un malintenzionato pubblicare una chiave facendosi passare per un altro o contraffare chiavi altrui, con o senza la complicità del gestore del registro, con il risultato che dalla massima sicurezza consentita dalla crittografia a chiave asimmetrica si passi alla massima insicurezza che deriva dalla malafede, o più semplicemente dalla negligenza, aggravate dall'impossibilità di distinguere i bit veri da quelli falsi.
Dunque, in tutto il processo della firma digitale è necessario l'intervento di una "**terza parte fidata**" (**trusted third part**), generalmente nota come **Certification Authority** (nel nostro ordinamento "**il certificatore**") che ha il compito di gestire il database delle chiavi pubbliche e dei relativi certificati delle chiavi ed ha la responsabilità di procedere all'identificazione del soggetto che richiede la certificazione.
L'insieme costituito dai soggetti indicati (utente, certificatore, destinatario, ecc.), il modo con il quale ciascuno di essi assolve al proprio ruolo e le modalità di utilizzazione delle tecnologie disponibili, costituisce la **PKI** (**Public Key Infrastructure**), l'infrastruttura di chiave pubblica.

3.5.3.2 ——— Le firme digitali automatiche e le firme digitali da remoto

L'utilizzo della firma digitale prevede che il titolare del certificato abbia la disponibilità materiale dello strumento di firma (solitamente una smart card o un token usb) e che la sottoscrizione avvenga solo dopo visualizzazione del singolo documento informatico da sottoscrivere.
Il CAD e le sue regole tecniche prevedono anche modalità di firma automatiche (senza obbligo di visualizzare ogni singolo documento) e con utilizzo del certificato da remoto. Tali procedure sono disciplinate dall'art. 35 del CAD e dal DPCM 30 marzo 2009, che ne specificano anche alcuni requisiti e impongono la garanzia di determinati livelli di sicurezza.
Il comma 3 dell'art. 35 del CAD stabilisce, infatti, che la firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima, poiché non si applica la disposizione di cui al secondo periodo del comma 2 dello stesso articolo, in base alla quale i documenti informatici devono essere presentati al titolare prima dell'apposizione della firma e occorre obbligatoriamente richiedere allo stesso la conferma della volontà di generare la firma.
Inoltre, ai sensi di quanto prescritto dall'art. 4, comma 2, del DPCM 30 marzo 2009, qualora il titolare del certificato di firma si serva di una procedura automatica di firma dovrà necessariamente utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso.
Con particolare riferimento all'effettivo funzionamento delle firme automatiche, occorre precisare che queste

non vengono realizzate mediante l'utilizzo dei comuni dispositivi forniti dai certificatori (token usb o smart card), ma si ricorre a strumenti tecnologicamente più avanzati e in grado di gestire più velocemente una maggiore quantità di dati. Al fine di garantire i livelli di sicurezza individuati dall'art. 35 del CAD, solitamente si ricorre all'utilizzo di sistemi particolarmente sicuri quali gli HSM (Hardware Security Module).
Per quanto riguarda, invece, le firme da remoto (server side), queste costituiscono una tipologia di firma elettronica avanzata o di firma digitale utilizzabile via web, nel quale la chiave privata del firmatario e il relativo certificato di firma vengono conservate da parte di un certificatore accreditato in un server remoto basato su un sistema HSM.
Nell'attuale disciplina delle firme digitali da remoto, sia il CAD sia le attuali regole tecniche contenute nel DPCM 30 marzo 2009 non vietano che i certificati possano essere generati su di un dispositivo remoto non posseduto direttamente dal titolare (come avviene mediante l'utilizzo di strumenti quali, ad esempio, la smart card o un token usb), ma impongono che il Titolare mantenga in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma.

3.5.3.3 —— Le firme elettroniche avanzate: le nuove regole tecniche

Le soluzioni di firma elettronica avanzata (FEA) sono state reintrodotte e regolate nel nostro ordinamento con le modifiche apportate dal D.lgs. n. 235/2010 al Codice dell'Amministrazione Digitale.
Attualmente, la normativa disciplina solo i requisiti fondamentali di tali tipologie di firma, presenti nella relativa definizione di cui all'art. 1, comma, lett. q bis) del CAD. Una firma elettronica avanzata, infatti, è quell'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Tuttavia, entro qualche mese dovrebbero essere approvate in via definitiva le nuove regole tecniche, la cui bozza è attualmente consultabile sul sito di DigitPa (www.digitpa.gov.it) e non dovrebbe aver subito modifiche rilevanti in fase di approvazione in sede nazionale e comunitaria.
Sulla scorta della bozza disponibile, le principali novità attengono all'assoluta libertà tecnologica lasciata agli sviluppatori di soluzioni di firma elettronica avanzata e all'assenza di qualsiasi controllo preventivo da parte della preposta autorità di vigilanza (dunque i soggetti che erogano sistemi di firma elettronica avanzata non sono soggetti ad alcuna registrazione).
In tal modo, si è inteso liberalizzare le tipologie di firma avanzata, non vincolandole più ad un certificato qualificato o ad un dispositivo sicuro, come invece richiesto per le firme elettroniche qualificate e per quelle digitali, entrambe species del genere firma elettronica avanzata.
Ciò in quanto le firme elettroniche avanzate, di norma, avranno un valore limitato al solo contesto in cui verranno utilizzate rendendo necessario che le loro condizioni di utilizzo siano preventivamente accettate per iscritto dagli utenti. Per questi motivi, il soggetto che propone l'utilizzo della soluzione di firma elettronica avanzata dovrà informare gli utenti in merito agli esatti termini e condizioni relativi al servizio, compresa ogni eventuale limitazione dell'uso.

Le soluzioni di firma elettronica avanzata non sono costituite da un determinato software, né da una determinata tecnologia, ma rappresentano un sistema neutro, sicuro e affidabile, idoneo a garantire la riconducibilità di un documento informatico, reso immodificabile, al soggetto che l'ha sottoscritto.
A tal fine, queste devono assicurare:

- l'identificazione del firmatario del documento;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
- la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- l'individuazione del soggetto di cui all'articolo 55, comma 2, lettera a);
- l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
- la connessione univoca della firma al documento sottoscritto.

Qualora i sistemi di firma elettronica in concreto adottati non dovessero assicurare i requisiti innanzi richiamati (ad eccezione della lett. f)) la firma elettronica generata non potrà soddisfare le caratteristiche previste dagli articoli 20, comma 1 bis, e 21, comma 2, del CAD, ossia qualità, sicurezza, integrità ed immodificabilità.
In generale, dall'art. 57 delle emanande Regole tecniche si evince che in capo ai soggetti che realizzano soluzioni di firma elettronica avanzata è posto l'obbligo di identificare in modo certo l'utente tramite un valido documento di riconoscimento, di informarlo circa gli esatti termini e condizioni relativi al servizio, compresa ogni eventuale limitazione dell'uso, di subordinare l'attivazione del servizio stesso alla previa sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente, conservando copia dei documenti di riconoscimento e della dichiarazione di accettazione delle condizioni d'uso relativi a ogni utente per almeno venti anni. Esclusivamente per le soluzioni di FEA utilizzate in ambito sanitario, il comma 5 dell'art. 57 delle nuove regole tecniche, prevede che la dichiarazione di accettazione delle condizioni del servizio da parte dell'utente possa essere effettuata anche oralmente.
In ogni caso, occorre tenere presente che tutto il processo relativo alla firma elettronica avanzata deve essere orientato alla sicurezza delle informazioni trattate. Inoltre, devono anche essere garantite l'integrità e la leggibilità dei dati e deve anche essere impedito ogni possibile accesso abusivo ai dati stessi (soprattutto quando i dati trattati siano di tipo biometrico). A tal fine, si consiglia l'adozione di standard internazionali relativi alla sicurezza delle informazioni trattate (ISO 27001).
Inoltre, è di estrema importanza che tutte le fasi del processo siano correttamente registrate e che i relativi log file siano conservati insieme ai documenti e a tutte le altre informazioni relative al processo di firma elettronica. Un idoneo sistema di conservazione, infatti, è in grado di garantire l'integrità dei dati oggetto di archiviazione e consentirà l'esibizione dei documenti e delle relative informazioni ad essi associati (informazioni che unitamente al documento di riconoscimento costituiscono la FEA).
L'art. 61 delle nuove regole tecniche, stabilisce anche che i messaggi inoltrati alla Pubblica Amministrazione tramite Posta Elettronica Certificata (quella - prevista dall'art. 65, comma 2, lett. c-bis del CAD - rilasciata

previa identificazione del richiedente da parte del gestore del servizio di PEC) e per i quali si sia richiesta una ricevuta completa, sono da considerare sottoscritti con firma elettronica avanzata.
Allo stesso modo anche soluzioni di FEA realizzate dalla PA e basate sull'utilizzo della Carta d'Identità Elettronica (CIE) o della Carta Nazionale dei Servizi (CNS) soddisfano i requisiti richiesti dalla normativa e rappresentano delle valide soluzioni di FEA.
Inoltre la normativa esclude, nelle soluzioni appena richiamate (basate su PEC, CIE e CNS) l'applicazione di alcuni limiti e di alcuni obblighi (quelli previsti dall'art. 57 comma 1 lett. da 1 a e e art. 58 commi 1 e 2 delle nuove regole tecniche) previsti per le altre soluzioni di FEA, riconoscendo la loro efficacia giuridica e probatoria anche nei rapporti giuridici con terzi soggetti (diversamente da quanto previsto dall'art. 60 delle nuove regole tecniche).
In ogni caso, successivamente all'approvazione definitiva delle Regole tecniche, l'Agenzia per l'Italia Digitale (che ha assorbito tutte le funzioni di DigitPa) pubblicherà delle apposite linee guida al fine di favorire la realizzazione di soluzioni di FEA conformi alle regole tecniche.

3.5.3.4 —— Le firme elettroniche autenticate

Un discorso a parte infine va, fatto sulla possibilità che un pubblico ufficiale autentichi una firma elettronica fornendole, in tal modo, un valore giuridico e probatorio tipico delle scritture private riconosciute (in pratica diventa impossibile il disconoscimento della sottoscrizione a meno che non si proponga un'apposita querela di falso).
L'articolo 25 del Codice dell'Amministrazione Digitale, così come sostituito dal D. lgs. 235/2010, infatti, prevede che si abbia per riconosciuta, ex articolo 2703 c.c., la firma elettronica o qualsiasi altro tipo di firma elettronica avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.
L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata, consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

3.5.4 —— Firme elettroniche applicate ai Documenti Clinici Elettronici (DCE) della CCE

Dal punto di vista archivistico la CCE è un fascicolo - e, quindi, come tale ha un'apertura, una chiusura e, ovviamente, un Responsabile - che contiene documenti di varie tipologie come indicato nei capitoli precedenti.
Relativamente al tema delle firme elettroniche dei DCE contenuti in una CCE, ogni azienda sanitaria dovrà, pertanto, definire: quali sono i DCE da sottoscrivere e il formato con cui sono rappresentati, quale tipologia di firma elettronica usare, quale formato nel caso di firma digitale.
È opportuno evidenziare che non vi sono norme che danno risposte precise in tal senso e, pertanto, ogni realtà deve trovare le risposte in funzione del suo specifico livello tecnologico-organizzativo.

Relativamente alla documentazione prodotta, esistono documenti quali l'anamnesi medica, i referti e le consulenze interne che si formano e si chiudono al termine della redazione da parte del medico. Questi documenti, che hanno una loro validità a prescindere dalla cartella clinica a cui si riferiscono, una volta completati devono essere firmati con firma digitale e trasmessi subito al sistema di conservazione digitale a norma, oltre che essere registrati all'interno della CCE.
Nella CCE vengono, inoltre, effettuate singole operazioni - anche ripetute nel tempo come, ad esempio, le prescrizioni e le somministrazioni, le richieste amministrative, ecc. - che costituiscono le registrazioni di documenti più organici quali il diario medico o quello infermieristico (in generale il diario clinico). Queste operazioni, analogamente a quanto avviene con la cartella clinica cartacea, con la sola sigla dell'operatore, si possono registrare e legare all'identificativo dell'utente che ha generato a sistema la registrazione, ottenendo in tal modo una sorta di sottoscrizione elettronica semplice - ma, con alcuni accorgimenti, anche avanzata - delle registrazioni effettuate. Ovvio che anche in questo caso dovranno essere previste nel sistema informatico delle "chiusure periodiche" che garantiscano l'immodificabilità delle registrazioni informatiche effettuate, da gestire sempre e comunque attraverso un sistema di conservazione digitale a norma.
Tra i DCE che afferiscono alla CCE di degenza medica e chirurgica, si suggerisce di firmare digitalmente almeno i seguenti:

- referti di esami strumentali (diagnostica per immagini, laboratorio di analisi, anatomia patologica, ecc.);
- referti di visite specialistiche;
- verbali di atti operatori;
- altri documenti ritenuti rilevanti dal punto di vista clinico e medico legale;
- lettera di dimissioni;
- Indice di chiusura della CCE.

In merito agli altri DCE afferenti alla CCE quali, ad esempio il diario medico e quello infermieristico, ogni Azienda deve trovare le migliori soluzioni che possano garantire la tracciabilità di chi ha fatto cosa e quando.
Ogni tipologia di firma elettronica deve tener conto degli aspetti operativi, di sicurezza e di economicità.
Ad esempio, come sopra sottolineato, le registrazioni cliniche possono essere sottoscritte con firma elettronica "semplice". In questo caso sarà però opportuno usare la strong authentication per accedere all'applicazione CCE e conservare i log file delle operazioni di firma.
Attualmente non esistono norme specifiche che prevedano un'associazione tra il tipo di firma elettronica e la tipologia del documento da sottoscrivere. I suggerimenti sopra riportati, pertanto, sono dettati dallo stato dell'arte tecnologico e dalla sostenibilità organizzativa. Si ritiene opportuno che ogni azienda sanitaria provveda a descrivere tale associazione nel Manuale di Gestione del protocollo informatico previsto dal DPCM 31-10-2000, laddove esista, o in altro manuale ad esso corrispondente per contenuti e finalità.
Per quanto riguarda, in particolare, la documentazione digitale della Diagnostica per Immagini, si rimanda alle Linee Guida del Ministero della Salute (Intesa Stato-Regioni 4-4-2012).

3.5.5 —— Formato elettronico dei DCE

Ogni azienda sanitaria dovrà definire, inoltre, il formato da usare per ogni tipologia di DCE afferente alla CCE.
Anche in questo caso non esistono attualmente precise indicazioni normative. È disponibile, anche se al momento in cui scriviamo si tratta solo di una bozza non ancora approvata definitivamente, un documento allegato alle "Nuove regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni" nel quale sono analizzati i formati attualmente più utilizzati, anche nel settore sanitario.
I formati di rappresentazione elettronica dei documenti possono essere macroscopicamente suddivisi in due categorie: una orientata alla comprensione umana (es.: pdf, tiff, …); l'altra, orientata all'elaborazione informatica (es.: HL7-CDA2, DICOM, …).
Il CAD prevede che il titolare di un certificato di firma digitale lo utilizzi per sottoscrivere documenti che vede e comprende, come ad esempio un documento in pdf. Tuttavia è riconosciuta l'importanza di usare documenti strutturati in ambito clinico. Quindi, anche nel caso del formati dei DCE, molte sono le scelte lecite e possibili adottabili dalle aziende sanitarie.
Il formato dei DCE attualmente più diffuso è il pdf con associati file xml contenenti i metadati. Esistono anche formati che usano CDA2 con all'interno un pdf e, recentemente, sta riscuotendo un certo successo l'uso di file pdf con iniettato all'interno una struttura CDA2.
Per quanto riguarda le immagini diagnostiche, invece, il formato consolidato a livello nazionale e internazionale è il DICOM.
La scelta del formato dei DCE e degli studi immagini è fondamentale per l'interoperabilità. Si ritiene opportuno, pertanto, suggerire alle aziende sanitarie di scegliere i formati da utilizzare tra quelli proposti da DigitPa, facendo riferimento alle eventuali linee guida e alle indicazioni della propria Regione, al fine di predisporsi in via prospettica anche alla realizzazione del FSE.

3.5.6 —— Formati di firma digitale dei DCE

Esistono tre formati di firma digitale: CADES (il classico formato pkcs@7, .p7m), PADES (firma pdf), XADES (firma xml).
Anche nel caso dei formati di firme digitali dei DCE, un'azienda sanitaria è chiamata a fare una scelta. Nuovamente il suggerimento alle aziende sanitarie è di scegliere formati di firma digitale, facendo riferimento alle LLGG o alle indicazioni della propria Regione, al fine di predisporsi strategicamente anche al FSE.

3.5.7 —— Modalità di apposizione della firma digitale

Un altro aspetto che gioca un ruolo rilevante nella dematerializzazione della CCE è scegliere con quale modalità firmare i DCE: firma "interattiva" (uno a uno), firma "a blocchi" (con una sola operazione vengono firmati più DCE) o firma "automatica" (attivata da un processo automatico).

Anche in questo caso la scelta deve essere attuata dall'azienda sanitaria in funzione del contesto tecnologico e organizzativo e in funzione dei DCE da sottoscrivere. Ad esempio i referti di visite specialistiche si prestano ad essere firmati in modalità interattiva mentre i referti di laboratorio si prestano ad essere firmati "a blocchi" o in automatico.

3.5.8 —— Supporto del certificato digitale

Il certificato di firma digitale viene rilasciato, necessariamente, su un supporto sicuro come prescritto dalla legge. Oggi si usano: smartcard, businesskey o HSM (Hardware Secure Module).

La scelta del supporto da utilizzare deve prendere in considerazione:
- gli aspetti organizzativi che devono essere predisposti per garantire il minor tempo di indisponibilità del certificato;
- il numero di titolari: con poche decine di titolari attualmente si suggerisce l'uso di smartcard, aumentando il numero di certificati può essere utile considerare l'uso di HSM;
- la necessaria compatibilità (hardware e software) del supporto e dei certificati con tutti gli applicativi software che utilizzano la firma digitale.

La scelta del tipo di supporto da utilizzare deve, altresì, tenere in considerazione il tipo di dispositivi hardware in dotazione al personale medico e infermieristico che operano nei reparti di degenza. Sarebbe opportuno nel caso di utilizzo di tablet, dotarsi di dispositivi di firma remota, anziché vincolarsi a prodotti hardware che siano in grado di interfacciarsi con smartcard. In questo senso anche l'usabilità risulta essere determinante ai fini della corretta scelta del tipo di supporto. Inoltre, è importante considerare che all'interno di strutture complesse come quelle ospedaliere è indispensabile predisporre una corretta gestione amministrativa dei certificati di firma utilizzati, nonché predisporre e approvare una policy che individui tutte le modalità di corretto utilizzo dei dispositivi di firma rilasciati ai vari operatori sanitari (medici, infermieri, ecc..).
Relativamente all'utilizzo di firme digitali, è consigliabile che sia la struttura ospedaliera a richiedere il rilascio dei certificati per i singoli titolari così da poterne mantenere sempre un controllo. In caso di licenziamento del medico, ad esempio, sarà la stessa struttura a poter richiedere la revoca del certificato e non dovrà rimettersi esclusivamente alla diligente condotta del medico che dovrebbe richiederne la revoca.
Tutti i certificati di firma digitale richiesti, inoltre, dovranno contenere specifiche limitazioni d'uso così da garantire sia la struttura sanitaria che il titolare del certificato da eventuali utilizzi fraudolenti.

3.6 —— Conservazione digitale della CCE

Prima di entrare nel merito delle regole e degli accorgimenti che devono essere rispettati nel processo di conservazione della CCE è necessario ricordare che la Circolare del Ministero della Sanità, n° 61 del 19 dicembre 1986 N. 900.2/ AG. 464/260 prevede che "Le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre che costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario".

Affinché la cartella clinica elettronica mantenga nel tempo lo stesso valore probatorio di quella cartacea, si rende necessario ed indispensabile un corretto processo di conservazione digitale.
Per quanto concerne la correttezza dei processi di conservazione dei documenti informatici, il Codice dell'Amministrazione Digitale stabilisce in modo chiaro che ogni documento, che per legge o regolamento deve essere conservato, può essere riprodotto e conservato su supporto informatico ed è valido a tutti gli effetti di legge (vedi art. 43, comma 1, del CAD che stabilisce che "I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71").
La riproduzione e relativa conservazione del documento devono essere effettuate in modo da garantire la conformità dello stesso all'originale e la sua conservazione nel tempo. Inoltre, qualora il documento venga generato e prodotto in origine in modalità informatica, è obbligatorio che la conservazione permanente avvenga con modalità digitali (art. 43, comma 3, CAD).
Più in generale, la conservazione digitale può essere definita come quel procedimento che permette di assicurare la validità legale nel tempo a un documento informatico - inteso come rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti - o a un documento analogico digitalizzato.
Per entrare nel dettaglio, il significato che si deve attribuire al processo di conservazione digitale di un documento informatico, è quello di garantire allo stesso, già correttamente formato le caratteristiche di autenticità, immodificabilità nel tempo ed integrità, attraverso l'utilizzo degli strumenti del **riferimento temporale** e della firma digitale del Responsabile della conservazione.
L'uso della firma digitale del Responsabile della conservazione si rende necessaria per la validazione del processo di conservazione, rendendo immodificabile l'insieme dei documenti od il singolo documento affidati alla sua custodia e responsabilità, mentre la validazione temporale permette di determinare temporalmente in modo certo sia l'affidamento sia di estendere la validità dei certificati di firma digitale.
Come per i documenti informatici in generale, anche per i documenti appartenenti alla CCE si rende necessario sviluppare un processo che sia rispettoso dei parametri fissati dalle Regole tecniche. In attesa dell'approvazione definitiva e della pubblicazione in Gazzetta Ufficiale della bozza delle nuove regole tecniche (Regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni) è necessario conformarsi a quanto richiesto dalla Deliberazione CNIPA n°11/2004.
In base dunque alla Deliberazione CNIPA n°11/2004, la conservazione digitale dei documenti informatici, anche sottoscritti (e la CCE ne è un chiaro esempio, essendo formata da documenti che, inoltre, possono essere sottoscritti con varie modalità e livelli di responsabili e/o da più attori), deve ovviamente avvenire su supporti idonei alla conservazione e avrà come processo finale a chiusura del ciclo, l'apposizione sull'insieme dei documenti di varia provenienza che la compongono (cartella di accettazione, referti, diario clinico, diario infermieristico,consensi informati, ecc) o su un'evidenza informatica che contenga necessariamente una o più impronte dei documenti o di insiemi omogenei o attinenti ad essi, della firma digitale e della marca temporale a cura ed opera del Responsabile della conservazione, certificando il corretto svolgimento del processo stesso, come dettato dall'art. 3 della Deliberazione CNIPA 11/2004.
Relativamente alla tempistica di conferimento al sistema di "archiviazione legale", occorre distinguere i singoli documenti prodotti e/o firmati digitalmente, che andranno conservati nel più breve tempo possibile, e la cartella clinica nel suo complesso, che andrà conservata successivamente alla sua chiusura (a seguito della formazione della SDO). A prescindere dalla conservazione o meno dei singoli elementi prima della chiusura della cartella clinica completa, dovrà essere comunque garantita la reperibilità e la leggibilità di ogni singolo documento contenuto nella cartella stessa, attraverso un processo di indicizzazione e catalogazione delle informazioni affluite nel sistema di conservazione.
Il Responsabile della conservazione digitale deve, inoltre, garantire la totale e pronta tracciabilità di tutte le operazioni che vengono effettuate durante l'intero processo. Ciò permette, infatti, di agevolare le operazioni di controllo e verifica che possono essere richieste ed effettuate dagli organi preposti e di mappare in modo univoco l'iter percorso dal documento o dall'insieme dei documenti. In ambito CCE questo ha enorme valenza in quanto è requisito stesso della conservazione della CCE che consente, senza ombra di dubbio od incertezza alcuna, di risalire ai vari soggetti che si sono interfacciati al sistema informatico dell'azienda, ricordando quanto possa essere eterogenea sia l'origine dei documenti che la tipologia di soggetti che, a vario titolo firmano il documento nativo.
L'art. 44 del CAD elenca, poi, i requisiti minimi necessari che un sistema di conservazione deve garantire per la corretta conservazione dei documenti informatici, ossia:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

b) l'integrità del documento;

c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e classificazione originari;

d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

Inoltre, il successivo comma 1-bis dell'art. 44 del CAD prevede che "Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza".
Prima di passare all'analisi di un preciso modello tecnico-organizzativo per la conservazione è utile riportare alcune specificazioni sul concetto di immodificabilità e integrità presenti nelle nuove regole tecniche sul documento informatico[20].
La bozza delle emanande regole tecniche, al comma 2 dell'art. 3, dispone che "il documento informatico assume la caratteristica di immodificabilità se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta ed accesso e ne sia garantita la staticità nella fase di conservazione".

[20] Bozza di Regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41 e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Inoltre nel successivo comma 4 dello stesso articolo, vengono elencate tutte quelle che sono le operazioni idonee atte a garantire le caratteristiche di immodificabilità e di totale integrità nel caso in cui, appunto, i documenti vengano formati tramite l'utilizzo di appositi strumenti software. Queste operazioni sono:

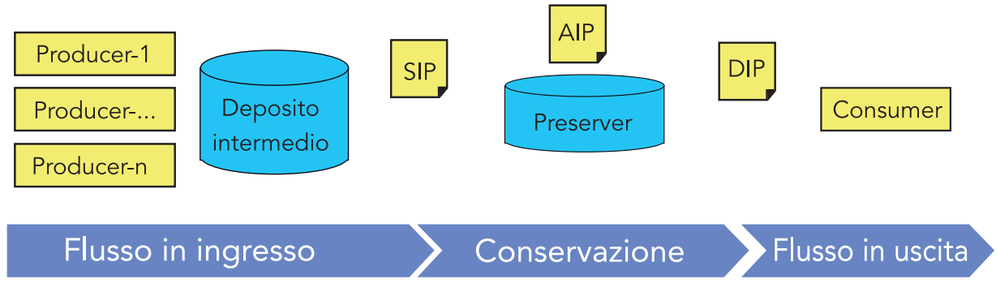
a) la sottoscrizione con firma digitale ovvero con firma elettronica qualificata;
b) l'apposizione di una validazione temporale;
c) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;
d) la memorizzazione su sistemi di gestione documentale che adottino politiche di sicurezza;
e) il riversamento in un sistema di conservazione.

Di particolare importanza è anche quanto previsto al comma 7 del sopracitato art. 3, il quale dispone che, ove non sia già presente, al documento informatico immodificabile deve essere associato un riferimento temporale (marca temporale), elemento che rientra comunque nell'elenco minimo dei metadati che devono essere associati al documento informatico immodificabile, in base al comma 9 dello stesso art. 3, insieme all'identificativo univoco e persistente, all'oggetto, al soggetto che ha formato il documento, nonché all'eventuale destinatario.
A questo proposito è fondamentale fare un inciso: nel caso di documento informatico acquisito per via telematica o su supporto informatico, o acquisito tramite copia per immagine su supporto informatico di un documento analogico, o ancora mediante copia informatica di un documento analogico, le caratteristiche di immodificabilità e di integrità sono determinate da quelle che sono le operazioni di memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità del documento o in un sistema di conservazione.
Nel caso di documento informatico formato tramite registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente, oppure mediante generazione o raggruppamento, anche in via automatica, di un insieme di dati o registrazioni, (provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

3.6.1 —— Implementazione tecnologico-organizzativa della conservazione della CCE (il modello OAIS)

È possibile scegliere differenti modelli per la creazione di un sistema di conservazione, purché siano rispettati i requisiti minimi richiesti dall'art. 44 del CAD citato.
Tra i vari modelli analizzabili, certamente il più interessante è il modello OAIS (Open Archival Information System). Tale modello costituisce lo standard ISO 14721 di riferimento per la certificazione dei depositi di conservazione. Tra l'altro lo standard OAIS è anche stato preso a modello per la redazione delle nuove regole tecniche per la conservazione.
La schematizzazione del modello OAIS, disegnata nella figura sottostante, è utile per comprendere quanto descritto successivamente nel presente documento.

Modello di riferimento OAIS (ISO 14721:2003)
Open Archival Information System



In particolare nella figura sono illustrati i concetti di:

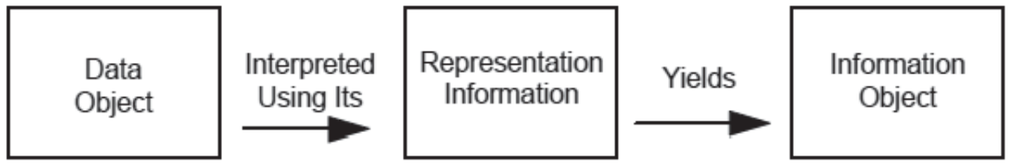
- flussi di ingresso: i flussi dei pacchetti informativi (SIP: Submission Information Package) dalle applicazioni che generano i documenti (Producer) e da eventuali depositi intermedi, quali ad esempio il Repository;
- sistema informatico di conservazione (Preserver) che si fa carico della conservazione dei documenti generati dai Producer, gestendoli in pacchetti informativi di archiviazione (AIP: Archival Information Package);
- flussi di uscita, comprendenti le funzionalità e/o le applicazioni (Consumer) che consentono l'accesso ai documenti conservati. I DIP (Dissemination Information Package) sono i pacchetti informativi usati per la distribuzione.

Nell'ambito delle CCE, per capire come posizionare la conservazione è opportuno rifarsi al modello OAIS.
I documenti informatici clinici contenuti in una CCE sono generati da un Producer (Produttore) e sono destinati ad uno o più Consumer (Utenti). Al fine di tutelare il percorso assistenziale e le responsabilità degli operatori e dell'azienda sanitaria è opportuno che i documenti prima di essere consultati siano stati conservati o quanto meno siano stati presi in carico dal sistema di conservazione (questo al fine di non rallentare i tempi di fruizione che in ambito clinico potrebbero introdurre delle criticità assistenziali). Questo flusso conferisce ai documenti una sorta di "certificazione" aziendale.
Dal punto di vista pratico e tecnico questa garanzia può avvenire implementando due possibili tipologie di flussi:

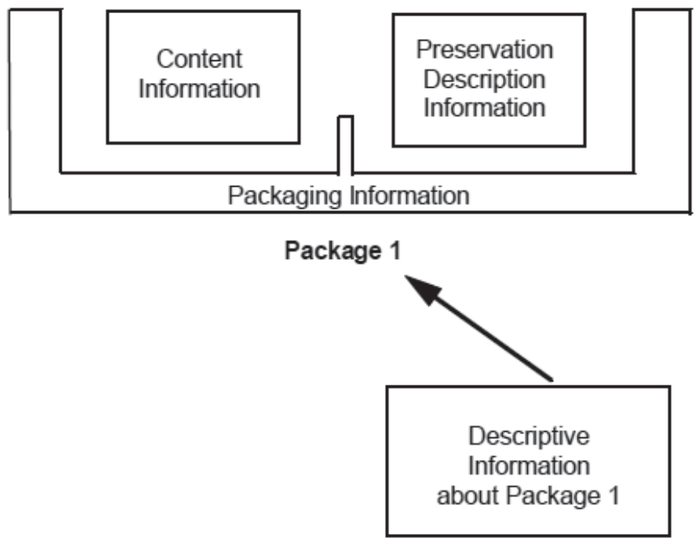
- Producer - Preserver (presa in carico) - Repository - Consumer;
- Producer - Repository - Preserver (presa in carico) - Consumer; si tenga presente che anche in questo flusso il consumer agisce solo dopo il preserver o meglio solo dopo l'avvenuta presa in carica dei documenti nel sistema di conservazione.

Non esiste in assoluto una scelta a priori. La tipologia di flusso da implementare, deve tener conto dello stato di informatizzazione corrente aziendale e delle sue necessità evolutive. In ogni modo, le scelte devono considerare l'interoperabilità interna ed esterna a livello interaziendale, regionale, nazionale e internazionale.
L'obiettivo principale di un modulo di conservazione è quello di consentire la conservazione a lungo termi-

ne dei documenti del repository documentale, in modo tale da garantire il mantenimento a lungo termine delle caratteristiche di integrità, autenticità, reperibilità, leggibilità, riproducibilità e trasferibilità. Inoltre, in conformità con quanto indicato dal modello OAIS, il modulo deve attuare la conservazione del documento non come la conservazione di un semplice oggetto informativo digitale, quanto di un pacchetto informativo costituito da informazioni di contenuto, informazioni di identificazione, informazioni di contesto, informazioni di provenienza, informazioni di stabilità, informazioni di pacchetto e dati descrittivi del pacchetto.
Il perno ovviamente di un archivio OAIS è il concetto di informazione, che nel sistema clinico-sanitario verrà rappresentata da una serie di dati, identificati dai documenti e dalle loro informazioni di rappresentazione all'interno del sistema e da una serie di documenti sanitari che dovranno essere gestiti singolarmente e non come un flusso documentale. La figura seguente, mostra la relazione del concetto di informazione vista proprio come un insieme di dati-oggetti.



Per conservare correttamente i dati del sistema clinico-sanitario e quindi le relative informazioni di interesse, sarà implementata una funzione di impacchettamento dell'intero Oggetto-dati e dei relativi documenti. In questo modo verrà a formarsi un pacchetto informativo che verrà individuato dal sistema grazie alle informazioni descrittive in esso conservate ed aggregate, come indicato dalla seguente figura:



Solo dopo che il contenuto dell'informazione è stato chiaramente definito sarà quindi possibile valutare la descrizione delle informazioni sulla conservazione, in modo tale che si preservino le informazioni, garantendo l'identificazione certa del dato e del documento e da chi è stata creata l'informazione su quello specifico contenuto. Questa soluzione permette anche di risolvere il problema relativo alla migrazione dell'intero archivio informatico di conservazione verso nuove tecnologie o cambiamenti nella gestione, nella struttura dei dati e nel formato dei files/documenti.
In tale contesto si richiama lo standard Cmis (Content Management Interoperability Services) attraverso il quale sarà possibile separare il contenuto informativo, dalle informazioni di conservazione (PDI), ambedue incapsulati e identificati dalle informazioni descrittive e soprattutto creare l'OAIS di conservazione-archiviazione. Si segnala in proposito che tale standard potrebbe non essere esaustivo data la peculiarità della conservazione digitale della documentazione clinica con particolare riferimento all'imaging, come verrà successivamente trattato.
Tale architettura logica, ci permette di fare le seguenti analisi:

- Le informazioni sulla conservazione sono l'insieme complessivo delle informazioni necessarie per la comprensione del contenuto informativo per un periodo di tempo indefinito; esso infatti deve includere le informazioni necessarie per conservare adeguatamente il particolare contenuto informativo al quale sono associate, garantendo che sia univocamente identificabile e che non abbia subito alterazioni. Avremo dunque quattro tipologie di PDI di conservazione: le informazioni sull'identificazione, che identificano gli attributi degli identificatori al contenuto informativo; le informazioni sul contesto, che documentano le relazioni tra il contenuto informativo e sanitario-clinico; le informazioni sulla provenienza, che forniscono e documentano le indicazioni sull'origine o sulla fonte del contenuto informativo, sui cambiamenti avvenuti dal momento della sua creazione e su chi ne ha curato la custodia sin dall'origine; le informazioni sull'integrità, che forniscono i controlli sull'integrità dei dati e le chiavi di validazione/verifica per garantire che il contenuto informativo non sia stato alterato.
- Tutte le funzionalità sopra descritte verranno implementate nel sistema sanitario-clinico, proprio tramite la veicolazione ed integrazione dello standard CMIS sopra descritto, che dunque permetterà di conservare in maniera sostitutiva, non un semplice oggetto informativo digitale, ma anche e soprattutto l'intero pacchetto informativo prodotto e i rispettivi documenti clinici prodotti.
- La soluzione proposta inoltre permetterà di fornire esaustive raccomandazioni che garantiscano che l'informazione archiviata nel modulo, resti accessibile sempre e comunque nel lungo termine anche qualora l'ambiente informatico d'origine diventi obsoleto.

3.6.2 —— La conservazione della CCE in outsourcing

La conservazione digitale è un processo complesso che richiede, per la sua realizzazione, strutture e competenze spesso non presenti all'interno dell'organizzazione a cui è richiesta la conservazione. Per tale motivo, il legislatore ha sempre esplicitamente ammesso la possibilità di affidare all'esterno parte o anche tutto il processo materiale di conservazione.
L'art. 44-bis del CAD stabilisce che "Il Responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto sta-

bilito dall'art. 42 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche".

La scelta relativa al se affidare o meno in outsourcing dev'essere attentamente valutata all'interno della struttura sanitaria che dovrà, inizialmente censire le proprie risorse umane e strutturali e, sulla base di questi risultati, valutare l'opportunità di affidare, anche solo in parte, il processo a soggetti esterni.

Già l'art. 5 della Deliberazione CNIPA riconosceva la possibilità dell'affidamento all'esterno così come l'art 44, comma 1-ter del CAD che, contestualmente, ha anche riconosciuto la possibilità che il titolare della documentazione da conservare, richieda, a soggetti terzi, la certificazione della conformità del proprio processo rispetto a quanto stabilito dall'art. 43 del CAD (Riproduzione e conservazione dei documenti) e dalle regole tecniche stabilite ai sensi dell'art. 71 del codice medesimo.

In merito a questo profilo, il successivo art. 44 bis prevede che i soggetti pubblici e privati, che svolgono attività di conservazione dei documenti e di certificazione dei relativi processi, possano accreditarsi presso DigitPa per conseguire il riconoscimento del possesso dei requisiti di livello più elevato in termini di qualità e sicurezza. La naturale conseguenza di tale disposizione è quella di rendere processualmente più problematico il disconoscimento di una copia digitale sostitutiva di un originale analogico effettuata da un conservatore accreditato.

L'accreditamento presso DigitPa (che sulla base delle nuove regole tecniche sarà indispensabile per quei soggetti privati che intendano offrire i propri servizi di conservazione alla PA) dovrà essere richiesto rispettando sia quanto previsto dal CAD sia quanto successivamente previsto da una circolare (la 59 del 2012) emanata da DigitPA.

Per concludere questo rapido excursus sull'outsourcing, è da considerare il fatto che la tendenza ad esternalizzare, propria di questo momento storico, non debba mai fare dimenticare che, la decisione di utilizzare questa modalità, debba essere unita ad una grande attenzione dal punto di vista delle gestione delle responsabilità, della Business Continuity e della implementazione corretta di SLA coerenti.

3.6.3 —— Considerazioni sulla conservazione della CCE in Cloud

Per ciò che riguarda il Cloud si ritiene sia da valutare in modo cautelativo una logica di tipo Cloud pubblico in un processo di conservazione, a norma, delle CCE. Oltre alle criticità relative alla protezione dei dati personali, si evidenzia anche una maggior difficoltà nella gestione della sicurezza nella conservazione dei documenti sanitari e clinici in un Cloud pubblico. Si ritiene invece essere maggiormente sostenibile, qualora sia scelta un'architettura ICT in Cloud di tipo SaaS o semplicemente come Web Application, riferirsi al Private Cloud.

Il private cloud è un'architettura proprietaria che fornisce servizi di tipo hosted a un numero limitato di utenti dietro un firewall e un load balancer. Difatti gli sviluppi nella virtualizzazione e negli ambienti distribuiti hanno permesso agli amministratori delle reti aziendali e dei datacenter di diventare service provider in ottica cloud che soddisfano le esigenze dei clienti all'interno dell'azienda stessa. Il Private Cloud può essere adottato da un'azienda che desidera o ha bisogno di maggior controllo sui propri dati rispetto a quanto farebbe utilizzando un servizio di terze parti come Elastic Compute Cloud (EC2) di Amazon o Simple Storage Service (S3).

In ambito sanitario, visti i maggiori requisiti che devono essere garantiti in materia di protezione dei dati personali e di sicurezza, potrebbe essere adottata una tecnologia di questo tipo per la conservazione delle CCE a condizione che vengano rispettati almeno i seguenti requisiti fondamentali:

- utilizzare solo ed esclusivamente un Cloud privato e quindi mai pubblico;
- rispettare gli standard fissati dalla normativa di settore;
- garantire la solidità tecnologica e di servizio nel tempo;
- consentire l'accesso ai dati, in entrata ed in uscita, in forma criptata, tipo PGP;
- implementare il processo di certificazione ISO 270001 o la ISO 20000:2005;
- implementare il processo di certificazione ISO/TS 21547:2010 per la gestione e la conservazione della cartella clinica elettronica e della documentazione sanitaria;
- applicare il Cloud in reti private e non reti pubbliche;
- verificare che la riservatezza dei dati memorizzati in Cloud, sia adeguata per la tipologia documentale trattata;
- avere una risorsa esperta nel cloud e non un sistemista di infrastrutture tradizionali;
- redigere uno SLA di riferimento adeguato solo per la nuvola;
- effettuare periodicamente e come indicato dalla normativa vigente, copie di back-up anche al di fuori della nuvola;
- virtualizzare solo e soltanto istanze cifrate dei propri application server;
- verificare la sicurezza dei meccanismi di clustering delle vostre applicazioni sulla nuvola;
- rendere persistenti i dati nella nuvola, per mezzo di storage a blocchi e snapshot cifrate.

In sintesi il procedimento di conservazione (non solo la parte tecnologica) deve garantire la conservazione dei documenti tenendo conto e governando il continuo e repentino cambio di tecnologie informatiche. Inoltre si deve tener conto che all'interno di un'azienda sanitaria i sistemi informatici clinici sono spesso molteplici per soddisfare esigenze di differenti branche cliniche e cambiano versione o fornitore, molto più frequentemente, rispetto al tempo di tenuta dei DCE da essi prodotti e sottoposti a conservazione.

È quindi importante approcciare la conservazione come quella "componente" che garantisce il patrimonio documentale dell'azienda sanitaria per i suoi fini strategici (assistenziali) prima ancora che un mero strumento di adempimento alla norma. Il procedimento di conservazione della CCE non può essere, quindi, avulso dalla tipologia dei documenti gestiti e dai processi clinici informatizzati: la conservazione è parte necessaria, importante della CCE ed é profondamente integrata alle altre componenti informatiche ed organizzative che gestiscono la CCE stessa.

3.6.4 —— Conservazione degli Studi Immagini Digitali

Un utile riferimento per approcciare il tema della conservazione degli Studi Immagini Digitali sono le "Linee Guida per la Dematerializzazione della Documentazione Clinica in Diagnostica per immagini - Normativa e Prassi" reperibile nell'ultima versione al link

http://www.statoregioni.it/dettaglioDoc.asp?idprov=10549&iddoc=35770&tipodoc=2&CONF=CSR

Si tratta di un documento molto interessante che offre moltissimi spunti per una corretta conservazione digi-

tale. Purtroppo il documento non è stato mai definitivamente approvato e, quindi, potrà essere utilizzato solo come utile guida.

Accanto ai temi legati al corretto trattamento dei dati personali, è necessario altresì garantire ai documenti/referti sanitari inseriti nella CCE la possibilità di verificarne, in qualsiasi momento, la provenienza, l'integrità e l'originalità o, quantomeno, la conformità all'originale. A tali problematiche ha cercato di rispondere anche il Ministero della Salute attraverso la predisposizione di apposite Linee Guida per la dematerializzazione della "**Documentazione clinica di laboratorio e diagnostica per immagini**"[21]. Tali Linee Guida hanno individuato tre tipologie di documenti sottoponibili al delicato processo di "dematerializzazione": il **referto**, le **immagini** e il c.d. "**referto strutturato**", individuando per ogni tipologia documentale i relativi tempi di conservazione e i soggetti responsabili di tale attività[22].

Su tali Linee Guida si è pronunciato anche il Garante Privacy attraverso un parere (Provvedimento del 26 novembre 2009) che ha avuto l'obiettivo di fornire le corrette indicazioni per poter gestire e conservare nel tempo la **documentazione clinica testuale e iconografica ottenuta direttamente in formato digitale**, nel rispetto delle attuali normative. In particolare, nel documento sono stati analizzati i molteplici aspetti relativi alla dematerializzazione della documentazione clinica e sono state individuate le soluzioni tecniche e organizzative ritenute più idonee ad avviare tale processo:

- individuare (per la memorizzazione dei dati) distinte soluzioni tecniche in funzione delle peculiarità e delle esigenze di ciascuna fase operativa, indicando per la fase di **archiviazione storica una conservazione in forma crittografata** o, in alternativa, l'impiego di **forme di anonimizzazione dei dati identificativi**, prevedendo altresì la creazione di profili differenziati per l'accesso ai due suddetti archivi e le necessarie procedure di autenticazione distinte per i vari profili individuati;
- nei casi di gestione in **outsourcing** del procedimento di conservazione dei referti (in ambito pubblico o privato), designare tale soggetto anche **responsabile del trattamento dei dati**, specificando analiticamente, nell'atto di designazione, sia le modalità di conservazione dei documenti, sia le misure di sicurezza da adottare (art. 29 e artt. 31 e ss., d. lgs. n. 196/2003);
- **sviluppare strumenti di audit ex post degli accessi agli archivi contenenti i referti**, sia nella fase di memorizzazione PACS, sia in quella di archiviazione storica, definendo un processo di management dei log che sia in grado di rappresentare con completezza, per una determinata profondità temporale opportunamente commisurata alle esigenze di controllo sul corretto utilizzo della base di dati e degli accessi da parte del titolare del trattamento, l'insieme delle operazioni effettuate sui referti e di garantire l'inalterabilità dei log memorizzati;
- creare **procedure tecnico-organizzative idonee a ridurre il più possibile**, nel processo di dematerializzazione dei referti, **l'incidenza di operazioni manuali** (es., l'associazione tra i resoconti del medico specialista e le immagini contenute nei referti, ovvero la titolazione dei volumi nella fase di archiviazione storica), in quanto caratterizzate da elevato tasso di errore.

[21] Il 4 aprile 2012 la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Provincie autonome di Trento e Bolzano ha sancito un'intesa tra gli enti citati in relazione alle "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini".

[22] Generalmente nella cartella clinica viene conservato il solo referto; tuttavia, se si tratta di referto strutturato è necessario conservare anche la relativa immagine, con le ovvie problematiche che ne derivano in tema di corretta conservazione.

3.6.5 —— L'indice di conservazione e la norma UNI SINCRO

La Deliberazione CNIPA 19 febbraio 2004, n. 11, recante le "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali" rappresenta il riferimento legislativo attualmente in vigore in tema di conservazione; la Deliberazione propone delle strategie mirate per realizzare la cosiddetta conservazione sostitutiva, un processo teso a garantire la corretta memorizzazione e conservazione nel tempo di documenti informatici su qualsiasi supporto.

Tale attività non esaurisce ovviamente il complesso di azioni, strategie e strumenti che complessivamente configurano il processo di conservazione a lungo termine, che non sarebbe possibile racchiudere complessivamente in una singola norma; tuttavia, si configura come un importante tassello di questo processo e come tale necessita di un'attenzione mirata non solo ad analizzarne e comprenderne le caratteristiche tecniche e funzionali, ma anche a inquadrarne il ruolo, ed eventualmente a specificarne i dettagli, nel più ampio contesto del processo conservativo e delle istanze di interoperabilità.

Le regole tecniche per la conservazione sostitutiva descrivono gli aspetti procedurali e indicano le responsabilità degli attori di questo processo, ma non forniscono dettagli tecnici sulle modalità di rappresentazione dei dati e documenti oggetto di conservazione, e non contengono alcuna specifica disposizione mirata a conseguire o a promuovere forme d'interoperabilità. Gli articoli 3 e 4 in particolare (dedicati alla conservazione sostituiva di documenti informatici ed analogici) si limitano a prescrivere l'uso della firma digitale e di un riferimento temporale per perfezionare il processo, con l'intervento del Responsabile della Conservazione eventualmente integrato o sostituito da quello di un pubblico ufficiale.

Tecnicamente l'obbligo è limitato all'apposizione della firma digitale e del riferimento temporale "sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi". Questa indicazione offre ampi margini d'interpretazione in sede applicativa e di conseguenza ha consentito la proliferazione di soluzioni tecnologiche assai diverse tra loro, a danno dell'interoperabilità fra i diversi sistemi sviluppati dal mercato.

La formulazione astratta voluta dal legislatore mira a non condizionare in alcun modo il mercato con scelte precostituite; tuttavia è importante sostenere soluzioni a supporto dell'interoperabilità, soprattutto all'interno dei seguenti scenari:

- *evoluzione dei sistemi* - I documenti archiviati devono in generale sopravvivere per molti anni, ben più dei sistemi hardware e software a cui sono affidati: l'assenza d'interoperabilità rende difficile e costosa la migrazione verso nuovi sistemi e soluzioni tecnologiche, vincolando di fatto i soggetti possessori di archivi digitali ai fornitori di servizi e alle loro scelte, con ciò limitando l'auspicabile fluidità delle dinamiche di mercato;
- *accesso ai documenti* - La necessità di poter esibire (per esempio in sede giudiziale, o a scopo di consultazione da parte degli aventi diritto) i documenti conservati non è solo un'esigenza dettata dalla Deliberazione CNIPA, ma anche un inderogabile requisito di un corretto processo conservativo: in assenza d'interoperabilità è inevitabile che la mera conformità degli archivi alle regole tecniche richieda laboriose perizie, non potendo fare affidamento su strumenti e standard di riferimento per leggere i dati generati da applicazioni ad hoc.

Per rispondere a queste situazioni l'UNI, attraverso un'apposita commissione (a cui hanno partecipato anche alcuni membri di AISIS e ANORC), ha promulgato lo standard "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SInCRO)" (standard UNI 11386 - Ottobre 2010).
Per integrare il tema della conservazione sostitutiva in maniera coerente nel più ampio contesto della conservazione a lungo termine, sostenibile solo attraverso la definizione di modelli, strategie e pratiche archivisticamente corretti e adeguati a garantire la portabilità nel futuro degli oggetti contemporanei, nel rispetto della loro identità e del loro sistema di relazioni, va ricordato che la conservazione a lungo termine degli oggetti digitali dipende fortemente dal contesto entro cui gli oggetti sono immersi. Pertanto la piena comprensibilità degli oggetti digitali nel futuro dipende da molteplici fattori (tecnici, logici e organizzativi, in primis) che devono quindi essere descritti e documentati, pena la perdita di significato (parziale o totale) degli oggetti. La corretta conservazione a lungo termine implica cioè la descrizione sistematica e puntuale di formati, linguaggi, protocolli e, più in generale, di qualunque componente tecnologica funzionale alla comprensione degli oggetti digitali.
È quindi raccomandabile, in generale, ove possibile, conservare oggetti digitali in chiaro, non cifrati e non compressi, poiché tale strategia diminuisce il numero dei vincoli cui gli oggetti digitali sono soggetti e, conseguentemente, delle ulteriori componenti che occorre sottoporre a lunga conservazione. Viceversa, la conservazione a lungo termine di oggetti cifrati o compressi richiede la descrizione e/o documentazione delle tecniche di cifratura o di compressione adottate, onde garantire nel futuro la piena comprensibilità degli oggetti digitali.
Per analoghi motivi è altresì raccomandabile l'adozione di norme tecniche nazionali e internazionali, tanto nei processi di formazione e gestione degli oggetti digitali quanto nelle attività mirate alle loro conservazione, non solo per ovvi motivi d'interoperabilità, ma anche perché, in ragione della persistenza e diffusione di tali norme, i processi possono essere più facilmente documentati e descritti.
Ciò premesso è opportuno, quindi, che il sistema informatico di conservazione generi e gestisca Volumi di Conservazione in formato conforme allo standard UNI SINCRO. Il Volume di conservazione (VdC) definito da UNI SINCRO è un'unità logica elementare, risultato finale di un processo di conservazione sostitutiva. Il VdC è composto logicamente da:

- uno o più file ai quali si applica unitariamente il processo di conservazione sostitutiva;
- l'indice di conservazione (IdC);
- gli indici di conservazione antecedenti, se l'indice di conservazione attuale è stato originato da questi.

In aggiunta ai precedenti elementi, il VdC può contenere ulteriori componenti, per lo più con finalità di carattere gestionale. Per maggiori dettagli soprattutto sul formato del file IdC si rimanda allo standard medesimo.
Relativamente alla tempistica di conferimento al sistema di "archiviazione legale", occorre distinguere i singoli documenti prodotti e/o firmati digitalmente, che andranno conservati nel più breve tempo possibile, e la cartella clinica nel suo complesso, che andrà conservata successivamente alla sua chiusura (a seguito della formazione della SDO). A prescindere dalla conservazione o meno dei singoli elementi prima della chiusura della cartella clinica completa, dovrà essere comunque garantita la reperibilità e la leggibilità di ogni singolo documento contenuto nella cartella stessa, attraverso un processo di indicizzazione e catalogazione delle informazioni affluite nel sistema di conservazione.

3.6.6 —— Esibizione CCE

Prima di affrontare la tematica dell'esibizione è opportuno fare alcune premesse. Le norme sulla cartella clinica impongono la completezza delle informazioni e la contestualità di annotazione di fatti clinico-assistenziali relativamente a ciò che accade dal momento dell'accettazione al momento della dimissione del paziente.
La norma impone anche che la cartella sia un unico punto di raccolta di tali informazioni in ragione alla necessità che i singoli atti clinico-assistenziali debbano potersi basare su quelli precedenti (visite, esami diagnostici, …) e costituire un "continuum" terapeutico-assistenziale.
Una gestione "unitaria" della Cartella tende a essere favorita da una gestione tutta analogica o tutta digitale della stessa. Tuttavia la realtà, e il CAD ne ha preso atto, prevede la gestione di fascicoli ibridi: in parte analogici e in parte digitali.
Questo scenario ibrido è quello che troviamo oggi nella stragrande maggioranza delle strutture sanitarie, dove alcuni documenti sono gestiti in modo dematerializzato ab-origine (tipici i referti di laboratorio e i referti e le immagini di radiologia). Troviamo quindi cartelle composte in parte da documenti cartacei e in parte da documenti informatici. Appare probabile che la fase di avvio dei progetti di CCE sia caratterizzata proprio da uno scenario ibrido. In tale contesto si suggerisce l'adozione di alcune procedure:

1. Formalizzazione - Descrivere nei documenti formali dell'azienda come sono costituite e gestite le cartelle cliniche.
2. Formare ed informare tutti gli operatori dell'azienda.
3. Predisporre opportune procedure di archiviazione (con idonei controlli di completezza).
4. Predisporre opportune procedure di esibizioni.

L'esibizione di una Cartella Clinica ad un Paziente viene fatta su sua esplicita richiesta a fronte della quale un'azienda deve fornire una copia conforme. Il cittadino può chiedere di averne una copia o cartacea o digitale (le norme sempre più spingono verso questo mezzo).
Si possono quindi presentare i seguenti possibili scenari relativamente alla produzione di una copia conforme di una cartella clinica:

Cartella Clinica Elettronica al 100%

- *Copia conforme digitale* – copia di tutti documenti della cartella su supporto digitale e produzione di un file indice con dichiarazione di conformità di un pubblico ufficiale (tipicamente gli stessi operatori della Direzione Sanitaria che si occupano di produrre le copie conformi analogiche);
- *Copia conforme analogica* – stampa di tutti i documenti della cartella e attestazione di conformità ai documenti informatici conservati in azienda.

Cartella Clinica Analogica al 100%

- *Copia conforme digitale* – digitalizzazione di tutti documenti della cartella, creazione di un file indice con dichiarazione di conformità sottoscritta da un pubblico ufficiale;
- *Copia conforme analogica* – fotocopia dei documenti della cartella e attestazione di conformità di un pubblico ufficiale.

Cartella Clinica Ibrida

- *Copia conforme digitale* – digitalizzazione dei documenti analogici, creazione di un file indice comprenden-

te tutti i documenti dematerializzati e tutti i documenti scannerizzati e firma di conformità di un pubblico ufficiale;

- *Copia conforme analogica* – stampa dei documenti dematerializzati e attestazione di conformità sia su documenti stampati sia sulle copie dei documenti cartacei con attestazione di conformità da parte di un pubblico ufficiale.

3.7 —— BIBLIOGRAFIA E RIFERIMENTI

"**Linee guida Regionali per la Cartella Clinica Elettronica Aziendale**" (codice documento: "CRS-LG-SIEE#02") Regione Lombardia / Lombardia Informatica S.p.A. - 29-02-2012.

"**Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SInCRO)**" UNI 11386 - Ottobre 2010

"**Progetto Doge**" Regione Vento / Arsenal

CAD - Decreto Legislativo 30 dicembre 2010, n. 235 – Codice dell'Amministrazione Digitale

Decreto legislativo 196/2003 – Codice per la Protezione dei Dati Personali

Linee guida in tema di Fascicolo sanitario elettronico (FSE) e dossier sanitario - Garante per la protezione dei dati personali - 16 luglio 2009

Prescrizioni in tema di Fascicolo sanitario elettronico (FSE) - Garante per la protezione dei dati personali – 16 luglio 2009

Linee guida in tema di referti on-line – Garante per la protezione dei dati personali - 19 novembre 2009

Linee guida nazionali sul Fascicolo Sanitario Elettronico - Ministero della Salute - 11 novembre 2010

Disegno di legge N. 2935 approvato dalla Camera il 28/09/2011 e trasmesso al Senato – Delega al Governo per il riassetto della normativa in materia di sperimentazione clinica e per la riforma degli ordini delle professioni sanitarie, nonché disposizioni in materia sanitaria

Linee Guida Ministero della Salute Diagnostica per Immagini

IHE profilo XDS.b

Anorc, Guida pratica su firme elettroniche e firme grafometriche, Edisef, 2012

Dominio AMPRPA Person Topic Specifica di Localizzazione Italiana

CPI Sviluppo di un modello di Cartella Paziente Integrata - Progetto Ministero della Salute

4 —— Governance di un progetto CCE

4.1 —— Introduzione

Appare indubbio che la realizzazione di un progetto di CCE oltre a prevedere la gestione di complesse interazioni culturali, organizzative, di modifica di skill professionali sia fortemente dipendente da un utilizzo estensivo e pervasivo di tecnologia informatica.

Negli ultimi tempi, l'interesse per la governance dei progetti di innovazione tecnologica è aumentato notevolmente. Ciò in parte è dovuto alla rapida crescita delle tecnologie che generano ambienti e decisioni più complesse; in parte per la doppia natura, organizzativa e tecnologica, dei progetti ICT; e in parte per una crescente consapevolezza che i progetti ICT possono facilmente "andare fuori controllo" e impattare sui costi, sui risultati e sull'andamento dell'ospedale e quindi sul raggiungimento dei suoi obiettivi strategici.

Un approccio di "governance" implica avere una visione organizzativa nella quale tutti gli attori implicati nell'andamento dell'ospedale o del progetto di CCE, tra i quali ci sono anche i pazienti, possano fornire gli input necessari per consentire un adeguato processo decisionale nell'attivazione di un progetto complesso e temporalmente non breve. Questo approccio tende a favorire la condivisione della strategia e dei risultati e fa si che gli attori al di fuori della funzione ICT percepiscano il reale valore dell'utilizzo delle tecnologie informatiche in ambito sanitario.

Per meglio capire cosa si intenda per governance di progetti caratterizzati da un considerevole utilizzo di tecnologia informatica, di seguito vengono proposte alcune definizioni:

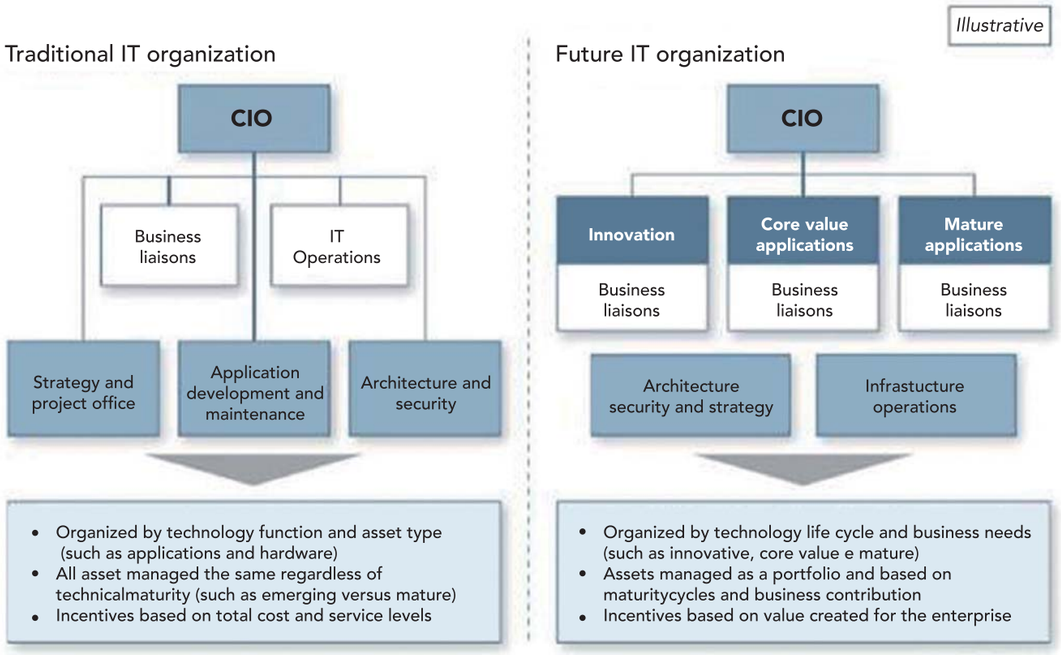
- L'Information Technology Governance Institute (ITGI) segnala che "la funzione che gestisce l'ICT (in termini di leadership, strutture organizzative e processi) deve essere in grado di favorire, sostenere ed estendere le strategie e gli obiettivi dell'azienda";
- Van Grembergen e De Haes (2009) definiscono la governace dell'ICT come parte integrante della "corporate governance" aziendale che affronta la definizione e l'attuazione di processi, dei meccanismi relazionali nell'organizzazione che consentono sia alle persone nelle aree di business sia a quelle nell'area ICT di eseguire le loro responsabilità a sostegno dei risultati d'azienda. In tale contesto si rafforza la necessità di una forte sinergia e allineamento tra strategia aziendale e strategia ICT, che il CIO deve in misura sempre maggiore favorire.

Indipendentemente dalla definizione, le tecnologie dell'informazione e comunicazione (ICT) devono essere gestite in modo coerente con gli obbiettivi e con le esigenze dei diversi attori che ne trarranno beneficio in un contesto di economicità e di generazione di valore per l'impresa e per i suoi clienti. Questo suggerisce l'opportunità di focalizzare l'attenzione sui seguenti ambiti:

- Allineamento strategico dell'ICT al business/attività dell'ospedale
- Generazione o possibilità di generare valore
- Gestione e mitigazione dei rischi associati all'utilizzo dell'ICT in sanità
- Gestione delle risorse in maniera efficiente e efficace
- Gestione operativa dell'attività

Per poter soddisfare questi obiettivi è necessario un cambiamento nel modo di concepire la funzione ICT aziendale che deve essere sempre più focalizzata ai processi di business e al conseguimento di risultati aziendali. Questo cambio faciliterà l'allineamento delle strategie operative a quelle aziendali consentendo una strutturazione dell'area ICT con ruoli ben definiti per aree e processi di business.

A strategic approach to technology management for tomorrow's IT organization
AT Kearney model for the IT organization



Appare necessario evidenziare che tale cambiamento culturale richiede anche un cambiamento organizzativo della funzione aziendale che si occupa di sistemi informativi su due versanti:

- un primo che riguarda la ricerca di equilibrio tra necessità di innovare e necessità di controllo. La funzione ICT deve essere, riprendendo le teorie di O'Relly e O'Connor, una struttura "ambidestra" vale a dire una funzione in grado di garantire stabilità e controllo ma anche di favorire l'innovazione. Purtroppo con una certa frequenza i professionisti dell'ICT vengono percepiti in azienda come coloro che "rendono difficile il facile passando per l'impossibile";
- un secondo che concerne l'organizzazione interna della funzione ICT aziendale (Agarwal e Sambamurthy, 2002) che dovrebbe essere fortemente orientata da un lato a coltivare "reti di relazioni" che consentano sia adeguate attività di demand management sia di favorire e di combinare conoscenze di utenti, direzione, fornitori nella classica catena del valore (Porter, 1994) dall'altro a favorire il processo di creazione del valore aziendale attraverso una focalizzazione/specializzazione oltre che sulle aree più propriamente tecnologiche anche sui processi di business primari (gestionali) e secondari (attività decisionali e di pianificazione strategica) considerando che i risultati in azienda si ottengono presidiando contemporaneamente tre variabili: Tecnologie, Processi (organizzativi e informativi) e Persone.

Appare evidente che queste scelte culturali e organizzative legate alla funzione ICT determinano anche un ripensamento legato agli skills e alle professionalità necessarie nell'affrontare progetti che richiedono da un lato un approccio progettuale e tecnologico di "enterprise architecture" (ad es. Project management, Revisione dei processi, architetture trasversali, standard di integrazione…) e nel contempo di concepire la funzione ICT in una logica di "service management" nella quale il focus dell'azione non è solo quello di assicurare un livello di funzionalità tecnologica ma quello di garantire una serie di servizi che consentono all'utente finale di poter utilizzare i sistemi informativi come supporto qualificante del proprio lavoro.

4.2 —— Governance dei progetti di CCE: requisiti, raccomandazioni e valutazione degli impatti

"Sviluppare e implementare un sistema integrato di condivisione dei dati del paziente è un progetto più difficile di quanto lo sia stato mandare l'uomo sulla Luna" (Collen Morris, 1995, Medical Director Division Technology Assessment - Kaiser Permanent).

Oggi sistemi ICT rapidi e attendibili rappresentano una componente vitale per un efficiente ed efficace "health management system" (Andreilla Vassiliou, EU Commissioner Health, 2011) e studi accademici e ricerche empiriche dimostrano che gli EMR sono il futuro della sanità (Kazley and Ozcan, 2007).

Tuttavia analisi sul campo hanno evidenziato che **tra il 50% e l'80% dei progetti di EMR falliscono** (Greenhalgh et al., 2009), o che l'implementazione dello stesso sistema di EMR in contesti diversi può portare a risultati estremamente differenziati e non sempre di successo (Nasi et al., 2010). Inoltre questi studi evidenziano che il successo di questi progetti dipende solo parzialmente dal software utilizzato mentre i risultati di successo sono correlati a una serie di pre-requisti di governance e di gestione complessiva di questi progetti.

Diverse sono le cause che non favoriscono il successo di questi progetti, tra cui le principali possono essere rintracciate nelle seguenti:

- assenza di una visione condivisa all'interno dell'organizzazione tra la Direzione Generale e gli stakeholders coinvolti relativamente agli obiettivi di revisione "trasversale" dei processi e dei dati clinici che progetti di CCE comportano;
- assenza di un'adeguata analisi organizzativa e dei processi che consenta di individuare i necessari cambiamenti per l'introduzione dei nuovi percorsi e delle nuove modalità di lavoro conseguenti all'implementazione di un sistema di EMR;
- assenza di un conseguente piano di change management e di formazione al cambiamento che progetti di questa natura comportano che tenga conto anche delle aspettative degli stakeholders coinvolti ma anche delle aspettative che, in ragione ad una condivisione trasversale dei dati clinci, non potranno essere soddisfatte. Nello specifico si evidenzia che con una certa frequenza si tende a confondere la necessaria attenzione alla formazione al cambiamento con la formazione tecnica che, pur necessaria e da pianificare con la dovuta attenzione ed estensione, non appare essere esaustiva;

- assenza di adeguate valutazioni sul mondo dei Vendor delle soluzioni EMR e della valutazione metodologica delle alternative sostenibili (vedi ad es. modello Gartner) mentre una forte partnership con il fornitore che consenta di conoscerne punti di forza e di debolezza, la roadmap degli investimenti e dei relativi sviluppi software, un coinvolgimento proattivo dello stesso che deve essere messo nelle condizioni di poter seguire adeguatamente lo svolgimento del progetto, appaiono requisiti che favoriscono la governance del progetto;
- assenza di un forte ruolo di project management che consenta di definire una specifica organizzazione di progetto:
  - l'individuazione dell'organigramma di progetto e dei K-user intesi come users che rispondono positivamente ai cambiamenti ed agiscono con proattività rispetto a quelli che sono contrari o subiscono passivamente i cambiamenti;
  - l'individuazione degli obiettivi del progetto, dei ruoli e delle responsabilità, del piano delle attività, dei risultati per ogni singola fase del piano;
  - la definzione di un adeguato piano di comunicazione interna come strumento di facilitazione dell'implemetazione del progetto;
- assenza di una dettagliata definizione dei risultati da raggiungere, delle metriche necessarie per la misurazione degli stessi, una valutazione sistematica con specifici strumenti di monitoraggio degli impatti del sistema CCE.

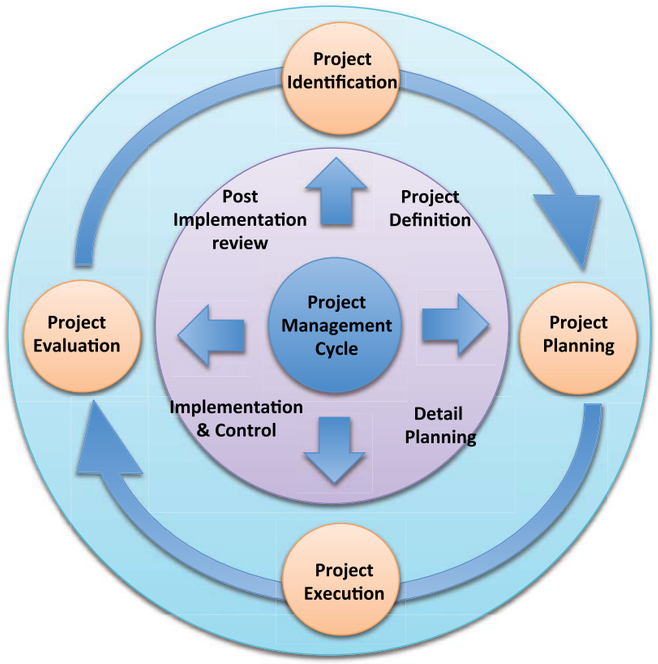
Di conseguenza è necessaria la definizione **di una strategia di governance** che consenta di gestire l'introduzione e l'implementazione di progetti di CCE. Alcuni elementi che dovrebbero caratterizzare la governance dei progetti CCE sono:

- **forte committment** da parte della direzione aziendale a sostegno di un'importante revisione sia dei processi organizzativi e culturali sia dei dati clinici entrambi in un'ottica di tipo "trasversale" al fine di ridurre l'iniziale resistenza verso questa tipologia di progetti che comporta significative modifiche culturali, di skill professionali richiesti, di processi organizzativi;
- **definizione del piano degli obiettivi di cambiamento** che si intendono raggiungere attraverso questo progetto di revisione dei processi e di condivisione trasversale dei dati clinici. Sua condivisione attraverso un adeguato piano di change management da attuare prima che il progetto venga avviato operativamente;
- **approccio partecipativo**, volto a promuovere la partecipazione degli stakeholders coinvolti sia nelle fasi di selezioni degli strumenti tecnologici sia nelle fasi di attuazione del progetto in quanto potrebbe ridurre la resistenza iniziale verso l'implementazione del sistema (Ovretveit et al. 2007). In tale contesto si evidenzia che la definizione di nuovi ruoli può aiutare nella produzione di risultati misurabili nel medio e lungo termine (Berg, 2009). Alcuni casi di successo hanno evidenziato che una co-gestione del progetto, attraverso l'affiancamento al Chief Information Officer di un Chief Medical Information Officer, ha oggettivamente favorito la condivisione degli obiettivi e dei risultati di progetto (Westbrook et al, 2009);
- **analisi organizzativa dei processi coinvolti** che consenta di definire, anche attraverso l'utilizzo di flowchart, lo stato dell'arte (as is) e le modifiche previste (to be) sia dei processi organizzativi sia delle informazioni ad essi connesse che il sistema dovrà garantire;
- **definizione dell'organigramma di progetto** definendo ruoli, responsabilità, livelli di coinvolgimento dei k-users, strumenti di gestione operativa del progetto e delle risorse strutturali, strumentali, organizzative e professionali, necessarie alla sua attuazione;

- **valutazione sistematica** del progetto e il sistematico monitoraggio degli impatti che il sistema CCE determina in quanto alcuni risultati potrebbero suggerire la natura e/o la direzione di possibili scelte strategiche/priorità dell'ospedale (Pagliari et al. 2005);
- gestione di leve motivanti per il cambiamento (es. incentivi) che consentano di persuadere anche i soggetti più ostili all'adozione di nuove tecnologie e nuovi comportamenti, alla collaborazione per il raggiungimento degli obiettivi condivisi.

4.3 —— Governance e fasi del progetto di CCE

In letteratura sono disponibili diversi modelli di Project Management Lifecycle. Di seguito ne proponiamo uno che tende a essere una sintesi dei vari modelli riprendendo anche quello del Project Management Institute del 1996.



Fonte: Aisis, rivisto da PM Lifecycle, Europaid Project Cycle Management Guidelines, 2004

Appare necessario in progetti complessi e articolati come quello della CCE dedicare particolare attenzione all'insieme di attività che devono essere assicurate in ogni fase del progetto al fine di garantire un'adeguata governance dello stesso. Nei paragrafi seguenti viene proposta una check list delle attività che si ritengono minimali per assicurare un'adeguata gestione delle fasi del ciclo di vita di un progetto di CCE. Ciò premesso, evitando inutili formalismi accademici nel seguito del documento verranno trattate tre fasi, unificando la fase di Identificazione e Pianificazione del progetto.

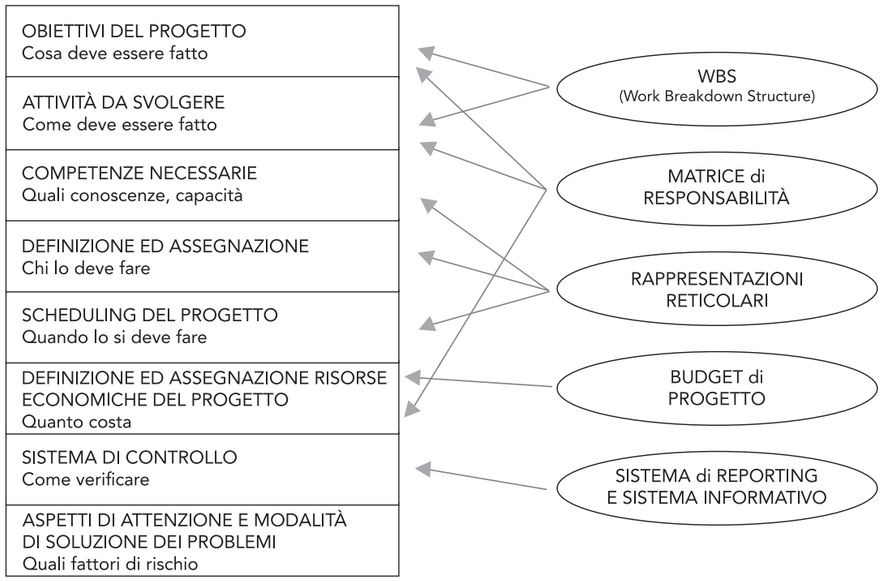
4.3.1 ——— Fase di identificazione e pianificazione del progetto: analisi dello scenario di contesto

Obiettivi e requisiti utili al successo del progetto

Obiettivo di questa fase consiste nell'analisi degli aspetti istituzionali, sociali, organizzativi, tecnologici, economico-finanziari, del quadro delle risorse necessarie per la realizzazione del progetto e ne determinano la "sostenibilità". Per sostenibilità si intende la concreta possibilità che in azienda esistano i requisiti sopraelencati per raggiungere i risultati di progetto in un tempo predefinito.
In questa fase appare opportuno predisporre un "documento di progetto" (o piano di progetto) nel quale definire in modo chiaro gli obiettivi che l'azienda intende perseguire con la realizzazione di un sistema di Cartella Clinica Elettronica. Questi obiettivi dovranno essere condivisi con la Direzione aziendale e gli stakeholders e adeguatamente comunicati a tutta l'azienda. Gli obiettivi potranno far riferimento a "economie di scala" (riduzione costi) o a "economie di scopo" (revisione dei processi e della loro qualità o revisione di servizi erogati). In tale contesto si segnala che la letteratura internazionale fornisce elementi incerti sulle economie di scala mentre tende a confermare vantaggi derivanti da economie di scopo in ragione sia di una revisione dei processi organizzativi, di una maggiore e più tempestiva disponibilità di informazioni clinico-assistenziali, di una maggiore trasparenza nel processo diagnostico-terapeutico-assistenziale determinata dal tracking delle attività resa possibile dai sistemi di CCE, di una maggior possibilità di audit clinico sui dati resi on line dai sistemi di CCE, sia della possibilità di offrire "servizi information intensive" anche ai pazienti come il download delle proprie informazioni cliniche per attività di second opinion o come supporto ai processi di continuità assistenziale, in una logica di patient empowerment.
Non si deve inoltre trascurare la necessità di armonizzare il progetto di CCE con gli scenari evolutivi previsti dagli ambiti sovra aziendali (es. regionali, nazionali) al fine di poter ottenere tutti i vantaggi di un approccio sinergico e condiviso. È utile infine attuare gli adeguati confronti a livello nazionale ed internazionale allo scopo di poter individuare i migliori orientamenti nella gestione informatizzata dei processi clinico-assistenziali.

Elementi caratterizzanti la governance (raccomandazioni)

Il documento di progetto deve contenere una serie di analisi che fanno riferimento alle aree indicate nella seguente slide:



Le attività da prevedere in questa fase sono almeno le seguenti:

1. identificazione degli stakeholders e dei k-users;
2. analisi di processo, definizione della relazione cliente/fornitore e definizione dell'architettura tecnologica;
3. pianificazione delle attività (almeno a livello macro);
4. determinazione del piano dei costi e delle risorse necessarie anche in termini di competenze;
5. valutazione dei rischi;
6. definizione dell'organigramma di progetto;
7. project charter e piano di comunicazione.

Identificazione degli stakeholders

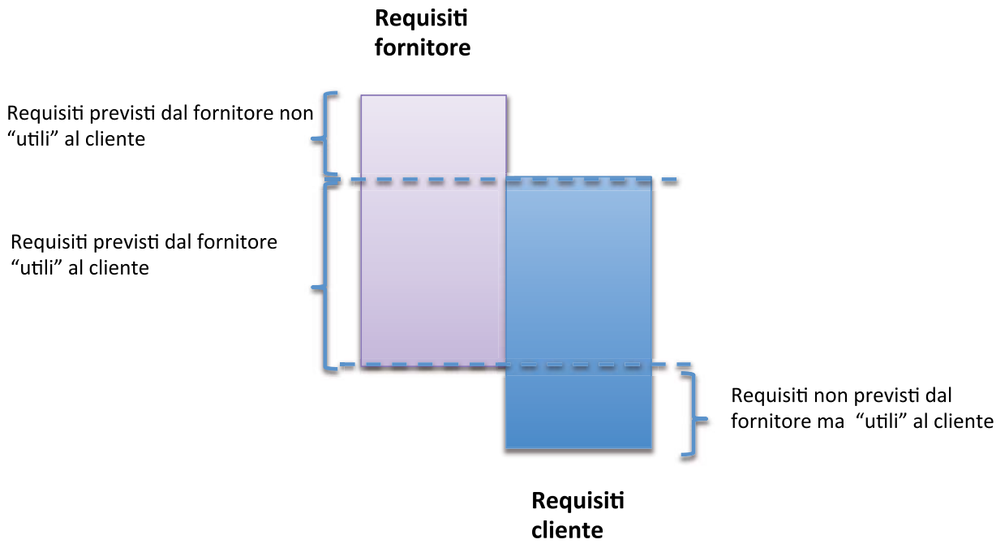
Gli stakeholders del progetto sono i "portatori di interesse" cioè coloro che trarranno beneficio dal fatto che il progetto riesca. Il concetto di "portatore di interesse" può essere più ampio del committente di progetto, infatti se da un lato il committente è certamente un portatore di interesse, un portatore di interesse può essere colui che può beneficiare dalla riuscita del progetto, ma non avere la possibilità di commissionare un progetto.
In ogni caso tutti i portatori di interesse hanno un duplice ruolo: possono determinare vincoli e caratteristiche, ma possono anche essere i motori che spingono verso la riuscita del progetto. In tale contesto è opportuno identificare la figura dei K-users che da un lato possono supportare il team di progetto nella definizione dei requirements che il sistema di CCE deve garantire ma contemporaneamente agire in modo proattivo per il sostegno e la diffusione del progetto.

Analisi dei processi e relazione cliente/fornitore

L'analisi dei processi attuali (as is) e la definizione dei processi "a tendere" (to be) rappresenta una tra le condizioni di successo/insuccesso dei progetti di CCE anche in ragione alla valutazione del gap esistente tra i due al fine dell'individuazione dei percorsi e delle attività da porre in essere per favorire il successo del progetto.
Questa fase richiede l'approfondimento di tre aree di indagine, come da schema seguente:

Per identificazione del processo si intende un'attività del team di progetto di definizione dei confini del processo, degli obiettivi del processo, una identificazione del process flow con indicazione dei tempi di ciascuna fase e degli stakeholders coinvolti in ogni fase. L'obiettivo è costruire una "mappa del valore" del processo "as is" e di confrontarla con la "mappa del valore" che verrà determinata dall'utilizzo del sistema di CCE.
In tale fase pare opportuno porre attenzione sia a una definizione dei processo organizzativo-gestionali sia alle dinamiche tra le varie figure professionali coinvolte.
Altrettanto importante appare una dettagliata analisi delle informazioni trattate, dei data set clinici gestiti, della documentazione clinica prodotta, dei fabbisogni informativi insoddisfatti con l'obiettivo di configurare un nuovo sistema di gestione automatizzata dei processi e delle informazioni necessarie al loro svolgimento.

Per relazione "cliente-fornitore" si intende un confronto tra i "requisiti cliente" determinati dall'attività precedente e requisiti previsti dal fornitore e resi possibili nel nuovo sistema CCE.
È presumibile che tra i due requisiti esista un gap.



Obiettivo di questa fase del progetto consiste nella ricerca di un equilibrio sostenibile sia rispetto alla normativa sia rispetto ai costi tra i due livelli di requisiti.
Si evidenzia, in questa fase di introduzione della CCE, la necessità di ipotizzare soluzioni "aziendali" di CCE di tipo "standard" con bassi livelli di "verticalizzazione" della soluzione tecnologica al fine di favorire una visione trasversale dei processi e di condivisione dei dati clinici che oggi rappresentano una delle criticità nella realizzazione dei piani diagnostico-terapeutico-assistenziali. Peraltro tale approccio consente una omogenea crescita culturale e tecnologica a livello aziendale nell'utilizzo di soluzioni informatiche complesse predisponendo l'azienda a successive azioni verso soluzioni totalmente filmless e paperless.

Pianificazione delle attività

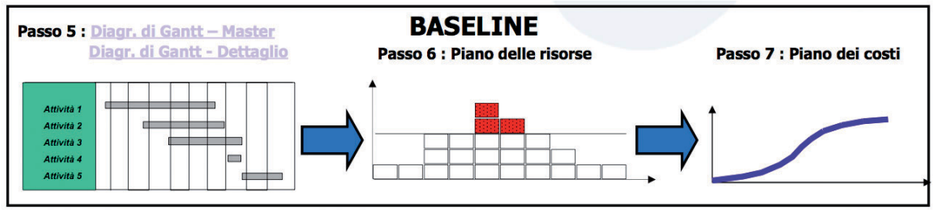
L'utilizzo della tecnica e di strumenti di WBS, acronimo di Work Breakdown Structure, di uso ormai comune nel Project Management, identifica una struttura gerarchica in cui il progetto viene scomposto in vari livelli, sino ad arrivare ad ottenere un elenco di attività, tra loro correlate, che è necessario compiere per realizzare il progetto (M. Damiani, 2007).
Questa tecnica è utile per individuare tutte le componenti del progetto e evitare duplicazioni, evidenziarne le correlazioni, definire associandole alle attività i livelli di responsabilità (chi fa cosa), i tempi (quando) e anche le risorse e i costi .
Non esistono WBS giuste o sbagliate, ma esistono WBS più o meno utili, vale a dire che sono in grado di far cogliere la complessità del progetto, la cui analisi periodica consente di verificare l'andamento del progetto, le attività critiche da monitorare che possono comprometterne e ritardarne i risultati, il rispetto dei tempi e in definitiva le azioni correttive da porre in essere. Non è quindi uno strumento di sola pianificazione del progetto ma di monitoraggio continuativo dello stesso.

Il Piano di progetto deve essere in grado di:

- Dare una visione realistica del progetto durante tutto il ciclo di vita
- Responsabilizzare tutti gli attori coinvolti su obiettivi specifici
- Evidenziare situazioni critiche e proporre valide alternative in modo tempestivo
- Tracciare un quadro previsionale dell'evoluzione futura del progetto
- Proporre e imporre una normativa comune a tutti gli attori coinvolti
- Assicurare la coerenza tra gli obiettivi parziali assegnati e quelli generali di progetto

Piano dei costi e delle risorse

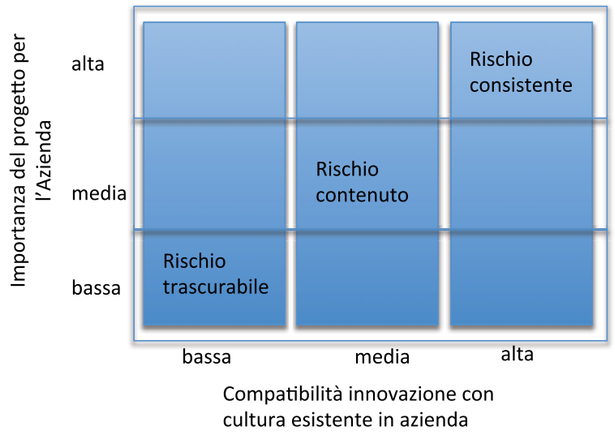
La definizione del budget di progetto è uno dei requisiti per una reale valutazione della sostenibilità dello stesso. Nella definizione del Budget dovranno esser indicate, in una logica pluriennale, sia i costi derivanti dal piano delle attività di cui al paragrafo precedente sia i costi generali di progetto (hw, sw, manutenzioni, consulenze, formazione).



Fonte: ripreso da M. Liguori, Uniroma corso economia e gestione delle imprese

Valutazione dei rischi

Nei progetti di trasformazione/innovazione organizzativa, come quello della CCE, si rivela di fondamentale importanza la verifica preliminare del livello di congruenza esistente tra la nuova strategia organizzativa e informativa proposta e il "livello culturale" che caratterizza l'Azienda nella sua globalità. Per stimare la dimensione del "rischio culturale", può dimostrarsi utile il ricorso al modello generale proposto da Schwartz e Davis che offre un semplice strumento di valutazione facilmente ed efficacemente utilizzabile nello specifico contesto.



L'utilizzo della matrice serve per condividere il rischio del progetto nel suo complesso e quindi i livelli di attenzione che lo stesso richiede a tutta la struttura aziendale. Maggiore il livello di "rischio culturale" stimato e maggiore dovranno essere il committment assicurato dalla Direzione Aziendale e le conseguenti azioni di monitoraggio del progetto da parte del team di progetto.

Se tutti i progetti andassero sempre secondo previsione non ci sarebbe la necessità di adottare tecniche di Project Management.
Nella realtà ogni progetto, piccolo o grande che sia, è soggetto a rischi che se non correttamente gestiti possono farne aumentare i costi, dilatare i tempi di realizzazione, pregiudicare la qualità del risultato. L'analisi dei rischi è finalizzata a mettere in relazione le diverse minacce alle quali è esposto il progetto con la probabilità per ciascuna di esse di potersi verificare e la gravità dell'impatto che l'evento potrebbe determinare. In proposito si suggerisce l'utilizzo di una matrice dei rischi che consenta una valutazione ex ante dei rischi e quindi stimoli l'attenzione e il monitoraggio delle variabili di rischio.

Impatto	Probabilità evento (1-4)	Rischi Organiz.vi	Rischi Piano Tempi	Rischi Tecnologici	Rischi Risorse	Rischi Finanziari
Molto grave	4					
Grave	3					
Medio	2					
Basso	1					

L'analisi dei rischi, che si suggerisce di svolgere mediante brainstorming con gli stakeholders, è complessivamente finalizzata a verificare l'esistenza di:

- aree di rischio non preventivate ma che si sono presentate nel corso del progetto;
- eventuali scostamenti (tempi, risorse, costi...) che possono compromettere il progetto;
- valutazione di azioni correttive;
- ri-pianificazione, qualora necessario, delle attività o di parti del progetto.

Definizione organigramma di progetto

La definizione dei livelli di responsabilità in progetto complessi come quello sulla CCE rappresenta un fattore critico di successo del progetto stesso. Tre elementi sono di particolare importanza: l'organigramma di progetto, la matrice delle responsabilità, la scelta del Project Manager.
Relativamente all'organigramma di progetto si suggerisce l'istituzione di:

- un Comitato di indirizzo (Steering Comitee) che deve rappresentare tutti gli stakeholders coinvolti e le relative istanze. In tale contesto si segnala l'opportunità della presenza di un rappresentante della Direzione strategica, della Direzione sanitaria, del Sitra, delle funzioni aziendali Sistema Informativo, Qualità e rischio clinico, Organizzazione (se struttura diversa dal SIA), Comunicazione e Marketing, Fornitore del sistema;
- un comitato di progetto che ha invece compiti di gestione operativa e monitoraggio del progetto tendenzialmente composto dal Responsabile del Sistema Informativo (CIO), un referente dell'area clinica (che svolga funzioni di Chief Medical Information Officer), un referente dell'area infermieristica, il fornitore.

In merito alla "Matrice delle Responsabilità" si suggerisce di chiarire ex ante quali sono i livelli di responsabilità dei vari stakehodlers presenti nel Comitato di indirizzo e nel Comitato di progetto e di formalizzare in una matrice che deve essere formalmente approvata (vedi esempio seguente meramente illustrativo).
La matrice delle responsabilità assolve sinteticamente tre importanti funzioni:

- ufficializzare formalmente le responsabilità dei vari attori evitando l'insorgenza del fenomeno "degli alibi";
- responsabilizzare gli attori del progetto sulle proprie responsabilità favorendone un approccio costruttivo;
- facilitare le attività di Project Management e il livello di trasparenza nella gestione del progetto.

Attività	**RU1**	**RU2**	RU3	**RU4**	**RU5**	**RU6**
Analisi	R	A	I	C	C	
Definizione	I	A	C			R
Gestione	R	A	I			S
Monitoraggio	R	A	I	C	C	S

- **R = responsabile**
- **A = approva**
- **S = supporta**
- **C = consultato**
- **I = informato**
- **V = verifica**

Al fine dell'individuazione del Project Manager si evidenzia che la scelta del PM condiziona fortemente il progetto e la sua realizzazione. Di conseguenza si segnalano alcune caratteristiche distintive per questo ruolo:

- **organizzativo-funzionali**: conoscenza processi organizzativi, conoscenza dei flussi informativi ad essi connessi e dello strumento informatico a disposizione, visione aziendale dei processi clinici e del progetto di CCE;
- **gestionali**: conoscenza delle metodologie di project management e di team building;
- **relazionali**: capacità di coaching, propensione al lavoro in team, capacità di sviluppare il potenziale del team e dei singoli che ne fanno parte, capacità di negoziazione e di relazione con la direzione e gli stakeholders;
- **personali**: flessibilità, capacità di comunicazione, propensione allla risoluzione dei problemi.

Project Charter

Il Project Charter rappresenta l'ufficializzazione del progetto che segue alla formale approvazione da parte

della Direzione Aziendale del documento di progetto. Non va considerato come atto formale ma come momento di presentazione di un progetto considerato "strategico" per l'Azienda. Deve consentire d'illustrare i motivi scatenanti del progetto, i principali obiettivi, i principali vincoli, i principali rischi. Rappresenta un momento di condivisione promosso dalla Direzione Aziendale per:

- ufficializzare l'avvio del progetto;
- formalizzare la delega al Project Manager e al team di progetto;
- chiarire a tutti il perché dell'avvio del progetto;
- ufficializzare gli obiettivi del progetto;
- permettere a tutti di riferirsi in maniera omogenea ed inequivocabile al progetto.

4.3.2 ——— Fase di attuazione del progetto

Obiettivi e requisiti utili al successo del progetto

A valle della fase di Project Charter il progetto viene avviato seguendo la WBS approvata. Lo scopo di questa fase è la realizzazione del progetto che viene assicurata mediante un livello di monitoraggio e controllo costante dello stesso. Il controllo è il processo che permette di garantire il conseguimento degli obiettivi generali dell'organizzazione e dei singoli obiettivi specifici. Si evidenzia in proposito che la gestione risulta ancora più complicata se alle complessità proprie del progetto si aggiungono anche frequenti e non preventivate richieste di personalizzazione o customizzazione.

Nel controllo, secondo la definizione di Megginson (1996), vengono effettuate delle analisi tra i risultati raggiunti ed i risultati che erano previsti in fase di pianificazione, vengono inoltre rilevati eventuali ritardi ricavabili dallo scostamento tra le date previste e quelle effettive ed inoltre vengono evidenziate (se esistono) le variazioni economiche dell'andamento del progetto registrate in corso d'opera. Il controllo in itinere consente di intervenire con rapide azioni correttive nel corso del progetto.

Elementi caratterizzanti la governance (raccomandazioni)

La fase realizzativa del progetto rappresenta la maggior criticità e richiede adeguate cautele e attenzioni.

Si suggerisce di presidiare sistematicamente e continuativamente le seguenti attività:

- monitoraggio dell'esecuzione delle attività di progetto tramite stati avanzamento lavori;
- eseguire stati avanzamento lavori sia con il Comitato di indirizzo (periodicità medio-lunga) sia con il comitato di progetto (periodicità medio-breve) con l'obiettivo di verificare il piano di attività, eventuali scostamenti, condividere eventuali azioni correttive. Ciò è possibile attraverso incontri, ispezioni, test, attività di audit;
- mantenimento di una rete di relazioni con tutti gli stakeholders coinvolti ivi comprendendo gli utenti finali;
- attivazione di un piano di comunicazione.

In merito al piano di comunicazione si evidenzia che la comunicazione, nelle sue varie forme e fini, è una attività chiave nella riuscita dei progetti e deve essere rivolta sia agli attori diretti del progetto sia agli stakeholder.

La comunicazione operata nei confronti dei vari attori che partecipano al progetto ha lo scopo di mantenere buona la performance di coloro che già stanno operando correttamente e di migliorare la prestazione di coloro che non stanno dando il meglio.

La comunicazione verso i portatori di interesse è indispensabile per mantenere le condizioni di conteso del progetto favorevoli. Coloro che non ricevono informazioni, a seconda delle propensioni personali, tendono ad enfatizzare le aspettative negative o quelle positive, entrambi atteggiamenti che danneggiano la conduzione di progetto. È bene quindi mantenere i diversi interlocutori aggiornati rispetto all'andamento del progetto con cadenze opportune, che sarebbe bene predefinire in maniera tale che non si creino false aspettative.

Può facilitare la sistematicità del piano di comunicazione l'adozione di una schema di riferimento come da modello riportato nello schema seguente:

Stakeholder/Attore	Tipo di informazioni da comunicare	Frequenza	Mezzo di comunicazione	Risultato della azione di comunicazione
[nome]	• [Tipo di informazione] • [Tipo di informazione] • [Tipo di informazione]	[giornaliera settimanale, mensile]	1. [mezzo 1] 2. [mezzo 2]	[descrizione]
[nome]	• [Tipo di informazione] • [Tipo di informazione] • [Tipo di informazione]	[giornaliera settimanale, mensile]	3. [mezzo 1] 4. [mezzo 2]	[descrizione]

Da ultimo si suggerisce l'opportunità di armonizzare il progetto di implementazione di un sistema EMR con le attuali esigenze di gestione dei processi clinico-assistenziali, i quali non nascono e si sviluppano esclusivamente in ambito ospedaliero bensì possono avere una componente preponderante della loro evoluzione nell'ambito territoriale/domiciliare. Il valore aggiunto del progetto potrà aumentare quindi al crescere della sua integrazione (o predisposizione all'integrazione) con le componenti territoriale/domiciliare dei processi di cura.

Nella fase di implementazione del progetto si ritiene opportuno segnalare due criticità che vanno presidiate: la modalità di adozione del sistema di CCE e l'estensione del progetto di CCE in realtà sovra-aziendali.

In merito alla prima criticità si segnala che da diverse ricerche empiriche emergono due modelli di adozione della CCE:

- un primo modello di attivazione "trasversale", ma in tutti i reparti, dei moduli che compongono la CCE iniziando da alcuni moduli (in genere i meno complessi come ad es. order entry e ricezione referti e immagini on-line) per adottare successivamente quelli maggiormente complessi (come ad esempio il ciclo del farmaco).

• un secondo modello che prevede l'attivazione "verticale" di tutti i moduli che compongono il sistema di CCE in uno o in un ristretto gruppo di reparti pilota.

Si evidenzia in proposito che, con una certa frequenza, l'attivazione del primo modello tende a garantire maggiori risultati principalmente per tre ordini di motivi:

• progressiva crescita culturale sia dei team medico-infermieristici coinvolti sia dei team ICT che possono congiuntamente valutare sul campo le esigenze, le criticità, le complessità da gestire adottando/affinando soluzioni organizzative e tecnologiche in tempi maggiormente rapidi;

• maggiore utilizzo del sistema proprio in ragione alla sinergia derivante dalla "trasversalità" della soluzione che consente una condivisione dei dati e dei processi clinici tra reparti e tra reparti e servizi diagnostici e/o di supporto;

• migliore e più rapido consolidamento e gestione dell'architettura tecnologica che "da subito" deve garantire affidabilità ma anche quelle integrazioni che sono alla base dei processi di continuità diagnostico-terapeutico-assistenziale che rappresentano uno dei principali obiettivi dell'utilizzo delle CCE.

Il secondo modello tende maggiormente a rispondere all'esigenza di "testare" tutto il percorso clinico, reso disponibile dalla soluzione di CCE adottata, in un reparto/dipartimento pilota. Nelle realtà dove è stato adottato questo secondo modello i rischi maggiori sono stati riscontrati proprio nell'eccessiva verticalizzazione del sistema, che rischia di dover essere riadattato al momento della sua attivazione in altri reparti (con costi e tempi incerti e crescenti), nella mancanza di sinergie di utilizzo del sistema dato che in fase di avvio tutta una serie di funzioni non potranno essere adottatte da tutti i reparti (ad es. consulenze tra reparti, gestione ambulatoriale...) che si accompagnano, con una certa frequenza, alla mancanza di integrazione con i servizi diagnostici. In sintesi l'attenzione al "particolare" tende a non consentire di raggiungere risultati "d'insieme".

Per quanto concerne la seconda criticità, in alcune realtà regionali è possibile che i progetti di CCE siano connaturati da un approccio sovra-aziendale che coinvolge necessariamente più ospedali (ad es. Estav, Federazioni). Se appare indubbia la possibilità di perseguire economie di scala, in tali situazioni è parimenti necessario che vengano definiti con chiarezza alcuni prerequisiti che possono garantire la sostenibilità del progetto:

• l'Owner del progetto vale a dire l'esatta identificazione di chi ha la responsabilità finale della gestione e dei risultati del progetto;

• i criteri di partecipazione dei vari stakeholders al progetto e i livelli di servizio che eventuali enti terzi devono garantire per la realizzazione del progetto. In tale contesto massima attenzione va dedicata alla matrice delle responsabilità;

• un piano di disarticolazione del progetto per singole strutture ospedaliere tale da consentire un monitoraggio costante dei vari sottoprogetti e, di conseguenza, del progetto complessivo.

4.3.3 ——— Fase di valutazione del progetto

Obiettivi e requisiti utili alla valutazione del progetto di CCE

Nei paragrafi precedenti si è già evidenziata la necessità di un monitoraggio sistematico del progetto che nei fatti consiste in una valutazione in itinere dello stato di attuazione dello stesso. Obiettivo di questo livello di valutazione consiste in una valutazione sistematica degli impatti del progetto sull'organizzazione nel suo complesso.

Elementi caratterizzanti la governance (raccomandazioni)

Nel merito della necessità di una valutazione sistematica si segnala che la **valutazione esclusivamente economica degli impatti prodotti dall'EMR** appare un metodo di misurazione del valore dell'ICT non adeguato in quanto non tiene in considerazione alcuni fattori strategici per l'incremento del valore per i clienti interni e finali. Occorre fare ricorso a modelli di valutazione che consentano di monitorare gli impatti che si manifestano in aree diverse, su orizzonti temporali diversi e in diversi ambiti aziendali e che rappresentino uno **strumento al servizio delle aziende** per rispondere in modo concreto ad alcune esigenze aziendali di valutazione del valore e degli impatti dell'adozione di innovazioni tecnologiche sui risultati e sulle performance aziendali.

Questo approccio di valutazione degli impatti di sistemi informativi fortemente innovativi richiede **un'adesione culturale a una logica di "performance management"** dell'innovazione tecnologica orientata alla valutazione continuativa del sistema e dei suoi effetti di breve e lungo periodo sull'azienda:

• è importante tracciare **la natura e direzione degli effetti nelle diverse fasi dell'implementazione** per apportare eventuali aggiustamenti o ritirare gli obiettivi;

• appare opportuno evidenziare che le esigenze interne maturano e si evolvono man mano che l'implementazione prosegue;

• si segnala il **benchmark** come strumento fondamentale per garantire alle aziende la possibilità di investigare i fattori che determinano il manifestarsi di taluni impatti in certi contesti e non in altri anche allo scopo di assumere al proprio interno azioni che ne facilitino la realizzazione.

In tale contesto si segnalano metodologie che consentono un'analisi del "valore aziendale" dei progetti di CCE reso possibile attraverso una valutazione multidimensionale degli impatti analizzandone i risultati ottenuti su diverse dimensioni: qualità, ottimizzazione delle risorse, efficacia organizzativa, empowerment del paziente (Nasi et al, 2009).

4.4 ——— Bibliografia di Riferimento

AA.VV. (2005), AT Kearney model for the IT organization, At Kearney Inc.

Agarwal, R. & Sambamurthy, V. (2002). Principles and models for organizing the information technology function. Minformation systems Quarterly Executive, 1(1), 1-16

Andreoulla Vassiliou, EU Commissioner Health (2009) eHealth, for a better quality of healthcare, in eHealth in Europe. The European Files May 2009 (17)

Berg, M. (2001) Implementing information systems in health care organizations: myths and challenges. International Journal Medical Information 64(2-3): 143-156

Black AD, Car J, Pagliari C, Anandan C, Cresswell K, et al. (2011) The Impact of eHealth on the Quality and Safety of Health Care: A Systematic Overview. PLoS Med 8(1): e1000387.

Caccia C., Cucciniello M., Nasi G., (2009), La valutazione degli impatti della cartella clinica elettronica, in Anessi Pessina E., Cantù E. (a cura di), L'aziendalizzazione della sanità in Italia.

Rapporto OASI 2009, Milano, Egea.

Collen, Morris F. (1995) A history of medical informatics in the United States, 1950 to 1990; in American Medical Informatics Association. Indianapolis.

Damiani M. (2007). Project Management di successo. Franco Angeli, Milano.

Greenhalgh T., Potts HWW, Wong G., Bark P., Swinglehurst D. (2009).Tensions and paradoxes in electronic patient record research: A systematic literature review using the meta-narrative method. Milbank Quarterly, 87(4), 729-88.

Kazley, A.S., and Ozcan, Y.A. (2007). Organizational and environmental determinants of hospital EMR adoption: a national study. Journal of Medical Systems. 31(5): 375-84.

Megginson, L.C., Nosley, D.C., Pietri, P.H. (1996). Management. Concetti e applicazioni. Franco Angeli, Milano

O'Connor G.C. and De Martino R. (2006). Organizing for radical innovation: An exploratory study of the structural aspects of RI Management Systems in large Firms. Journal of Product Innovation Management, 23, 475-497.

O'Reilly, C. A. III. and M. L. Tushman (2004). The ambidextrous organization. Harvard Business Review (April): 74-81.

Ovretveit, J., Scott T., et al. (2007a). "Implementation of electronic medical records in hospitals: two case studies" Health Policy 84: 181-190.

Ovretveit, J., Scott T, et al. (2007b). "Improving quality through effective implementation of information technology in healthcare." International Journal for Quality in Health Care 19(5): pp. 259-266.

Pagliari C, Sloan D, Gregor P, Sullivan F, Kahan J, Detmer D, Oortwijn W, MacGillivray S. (2005) What is eHealth (4): a scoping exercise to map the field. Journal of Medical Internet Research 7(1):e9.

Pinto, J.K., (1998). The Project Management Institute Project Management Handbook. Jossey-Bass, San Francisco, CA.

Project Management Institute (1996). A Guide to the Project Management Body of Knowledge. Project Management Institute, NC, Usa, 1996.

Porter, M. (1985), Competitive Advantage: creating and sustaining superior Performance, Free Press, New York, 1985.

Schwartz, H., & Davis, S. M. (1981). Matching corporate culture and business strategy. Organizational Dynamics, 10(1): 30–48.

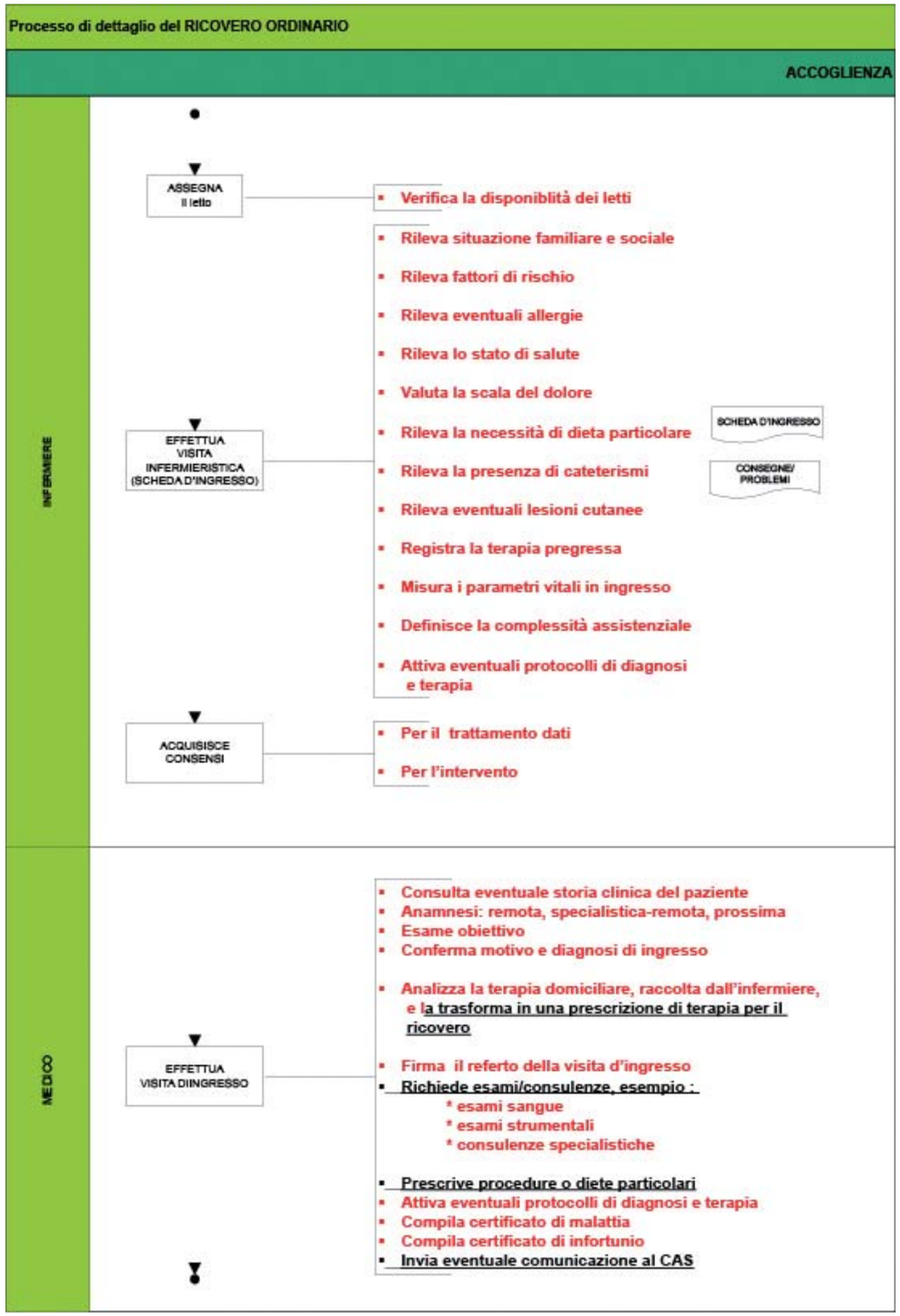
Van Grembergen, W., and S. De Haes (2009). Enterprise Governance of IT: Achieving Strategic Alignment and Value, Springer, 2009.

Westbrook, J., Braithwaite, J., Gibson, K., Paoloni, R., Callen, J., Georgiou, A., Creswick, N., Robertson, L. (2009), Use of information and communication technologies to support effective work practice innovation in the health sector: a multi-site study. BMC health services research. 9, 201.

5A Appendice X1 —— Mappe dei processi

1. Casella tratteggiata: rappresenta delle parti di processo che possono essere svolte o meno, a seconda del caso

2. Testo in nero e sottolineato: parti di processo che sono richiamate da più punti del processo complessivo



Processo di dettaglio del RICOVERO ORDINARIO

DEGENZA

INFERMIERE

GESTISCE LA DEGENZA del singolo paziente

- **Somministra le terapie**
- **Effettua le procedure e le medicazioni**
- Rileva parametri vitali
- Applica i protocolli
- Prescrive (prenota) i pasti in base alla dieta prescritta
- Aggiunge note
- Controlla le richieste (es: esami, consulenze) inviate
- **Rileva e gestisce eventuali problemi**
- Esegue i prelievi ematici e li invia al laboratorio

GESTISCE Le attività trasversali di reparto

- **Prepara le terapie**
- **Rileva e gestisce eventuali problemi**
- Gestisce i posti letto
- Gestisce l'approvvigionamento del magazzino di reparto

MEDICO

GESTISCE LA DEGENZA

- Consulta il diario clinico
- Consulta eventuale storia clinica del paziente e la visita d'ingresso
- Consulta gli esiti degli esami e i referti delle prestazioni diagnostiche ed eventuali consulenze
- Consulta il programma delle consegne
- Aggiunge:
  - * note cliniche
  - * relazioni
- **Richiede esami/consulenze, esempio :**
  - * esami sangue
  - * esami strumentali
  - * consulenze specialistiche
- Richiede emocomponenti (banca del sangue)
- **Richiede procedure**
- **Prescrive terapie**: infusionale, iniettiva, antimicotica, del dolore, nutrizionale, ecc.
- **Rileva eventuali problemi**
- Prescrive eventuale dieta personalizzata
- Programma eventuali interventi successivi

GIRO VISITA

- Conferma la prescrizione, l'informazione transita nella parte delle consegne

Processo di dettaglio del RICOVERO ORDINARIO

DIMISSIONE

INFERMIERE

COLLOQUIO ALLA DIMISSIONE

- Illustra i consigli alla dimissione
- Illustra la terapia domiciliare
- Raccoglie dati sullo stato del paziente necessari per i documenti di continuità assistenziale
- Libera il letto

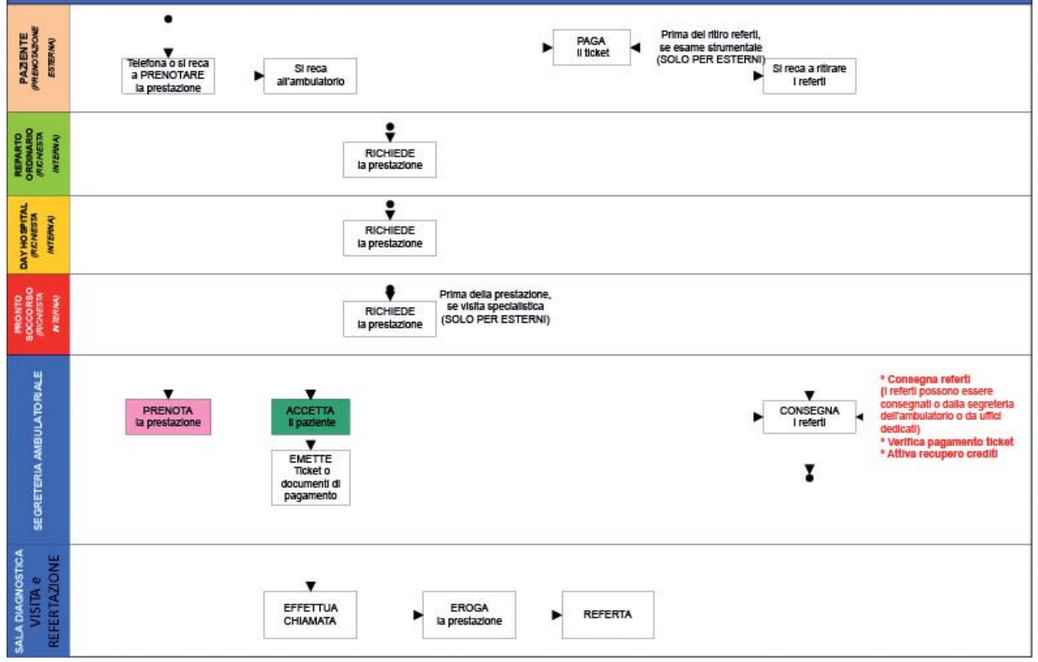
MEDICO

DIMETTE

- Redige lettera di dimissione
- Indica la modalità di dimissione (ordinaria, deceduto, ADI, volontaria, ecc.)
- Compila SDO
- Codifica SDO
- Calcola DRG
- Programma eventuale trasferimento
- Prescrive eventuale terapia domiciliare
- Programma prestazioni post ricovero
- Redige i documenti per la continuità assistenziale

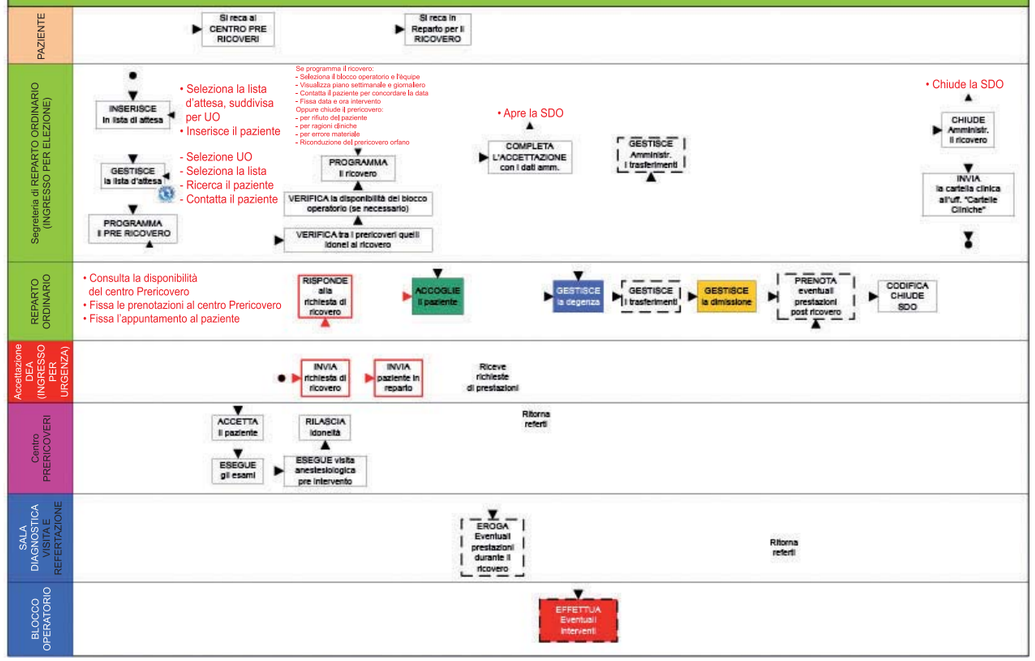
MACRO PROCESSI ospedalieri

PROCESSO: GESTIONE delle PRESTAZIONI AMBULATORIALI



MACRO PROCESSI ospedalieri

PROCESSO: RICOVERO ORDINARIO



Quadri Sinottici Ospedalieri

SINOTTICO CARTELLA CLINICA / DEGENZA PAZIENTE

Ingresso

(del Reparto Ordinario, PS, DH, DS, Dialisi) → VISITA d'INGRESSO / SCHEMA DIALITICO (Dialisi)

- Consulta eventuale storia clinica del paziente
- Anamnesi: remota, specialistica-remota, prossima
- Esame obiettivo
- Conferma motivo e diagnosi d'ingresso
- Analizza la terapia domiciliare, raccolta dall'infermiere, e la trasforma in una prescrizione di terapia per il ricovero
- Firma il referto della visita d'ingresso
- Richiede esami/consulenze, esempio:
  - Esami sangue
  - Esami strumentali
  - Consulenze specialistiche
- Prescrive procedure o diete particolari
- Attiva eventuali protocolli di diagnosi e terapia
- Compila certificato di malattia
- Compila certificato d'infortunio
- Invia eventuale comunicazione al CAS

(del Reparto Ordinario, PS , DH, DS, PRERICOVERI) → SCHEDA d'INGRESSO / TRIAGE (PS)

- Rileva situazione familiare e sociale
- Rileva fattori di rischio
- Rileva eventuali allergie
- Rileva lo stato di salute
- Valuta la scala del dolore
- Rileva la necessità di dieta particolare
- Rileva la presenza di cateterismi
- Rileva eventuali lesioni cutanee
- Registra la terapia pregressa
- Misura i parametri vitali in ingresso
- Definisce la complessità assistenziale
- Attiva eventuali protocolli di diagnosi e di terapia

Gestione giornaliera

(del Reparto Ordinario) → GIRO VISITE

- Consulta il diario clinico
- Consulta eventuale storia clinica del paziente e la visita d'ingresso
- Consulta gli esiti degli esami e i referti delle prestazioni diagnostiche ed eventuali consulenze
- Consulta il programma delle consegne
- Aggiunge:
  - note cliniche
  - relazioni
- Richiede esami/consulenze, esempio:
  - esami sangue
  - esami strumentali
  - esami strumentali
- Richiede emocomponenti (banca del sangue)
- Richiede procedure
- Prescrive terapie: infusionale, iniettiva, antimicotica, del dolore, nutrizionale, ecc.
- Rileva eventuali problemi
- Prescrive eventuale dieta personalizzata
- Programma eventuali interventi successivi

→ GESTIONE PROBLEMI

- Solleva problemi
- Prende in carico
- Risolve

(*diverso per PS) → ATTIVITA' per la DEGENZA del singolo paziente

- Somministra le terapie
- Effettua le procedure e le medicazioni
- Rileva parametri vitali
- Applica i protocolli
- Prescrive (prenota) i pasti in base alla dieta prescritta
- Aggiunge note
- Controlla le richieste (es. esami, consulenze) inviate
- Rileva e gestisce eventuali problemi
- Esegue i prelievi ematici e li invia al laboratorio

(*diverso per PS) → ATTIVITA' trasversali di reparto

- Prepara le terapie
- Rileva e gestisce eventuali problemi
- Gestisce i posti letto
- Gestisce l'approvvigionamento del magazzino di reparto

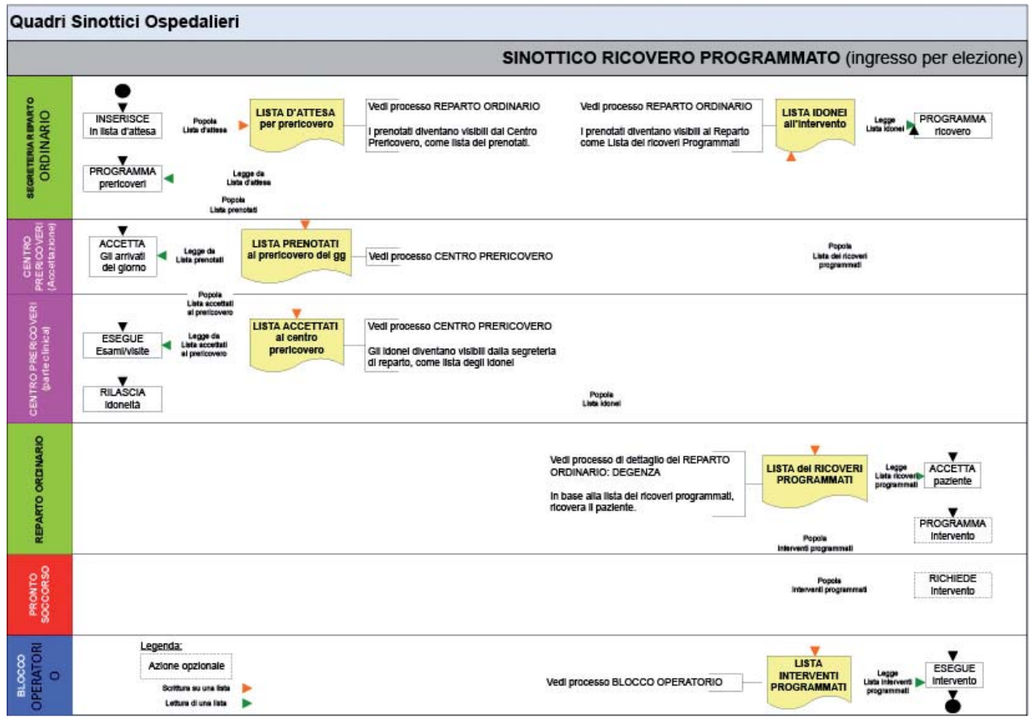
Dimissione

→ DIMISSIONE

- Redige lettera di dimissione
- Indica la modalità di dimissione (ordinaria, deceduto, ADI, volontaria, ecc.)
- Compila SDO
- Codifica SDO
- Calcola DRG
- Programma eventuale trasferimento
- Prescrive eventuale terapia domiciliare
- Programma prestazioni post ricovero
- Redige i documenti per la continuità assistenziale

→ COLLOQUIO alla DIMISSIONE

- Illustra la terapia domiciliare
- Raccoglie dati sullo stato del paziente necessari per i documenti di continuità assistenziale
- Libera il letto



6A Appendice X2. ——— Linee Guida per l'ICT Governance

Alcune linee guida di riferimento secondo la strutturazione di aree ICT

Categoria	Tipo	Linee Guida
IT Governace	Focus su come gestire le informazioni e le tecnologie dell'informazione e della comunicazione in modo efficiente ed efficace.	CobiT, ISO 38500, Val IT
Information e Service management	Focus su come eseguire e organizzare la gestione IT, come ad esempio la fornitura di servizi e supporto	Generic Framework for Information management, ITIL
Quality management	Focus su standard di qualità, applicato a specifici domini IT	TQM, ISO 9000, ISO 10006, ISO 20000, ISO 27001
Quality improvement	Focus sul miglioramento dei processi e della performance	IT BSC, ITS-CMM, Six Sigma
Project management	Focus sul portfolio, programma e gestione del progetto	MSP, PMBOK, PRINCE2
Gestione del Rischio	Focus su identificazione e gestione del rischio	ISO 31000, M_o_R, OCTAVE, FIRM

Linee guida per ogni disciplina che supporta la ICT Governance:

Governance Area	Linee Guida
Business service management	ITIL, Val IT
Business technology optimization	COBIT, Theory of Constraints, Val IT
Enterprise architecture	Zachman Framework
IT asset management	ITIL, Val IT
IT portfolio management	Val IT
IT Risk management	M_o_R, OCTAVE
IT security assessment	ISO 27001
IT service management	ISO 20000, ITIL
Project and program management	MSP, PMBOK, PRINCE2
Project governance	Val IT
Quality management	ICT Balanced Scorecard, CMMI, ISO 9000, TQM

Hanno reso possibile la pubblicazione del presente documento
e la realizzazione del convegno annuale Aisis 2012