
# Codice di condotta per la protezione dei dati personali in sanità

*Nota*

*I Capitoli da 1.1. ad 1.4 di questo documento sono già stati oggetto di verifica del consenso da parte dei partecipanti all'iniziativa (come riportato nel doc. 178/1018 del 7.10.2018) e comprendono i contributi e le integrazioni fornite in quella sede.*

*I Capitoli da 1.5 ad 1.9 descrivono -in termini di finalità, dati necessari e criteri di abilitazione- le altre tipologie di trattamento di dati personali implementabili nelle organizzazioni sanitarie. Su tali capitoli si richiede di esprimere il consenso ed eventuali contributi mediante il modello definito nel doc. 183/1018 del 14.10.2018*

## Premessa

Le strutture e le esigenze delle organizzazioni sanitarie sono molteplici, sia per la varietà dei contesti organizzativi (individuali, locali, territoriali), sia per la molteplicità delle patologie e forme assistenziali, ognuna delle quali con possibili requisiti specifici, sia per la varietà delle esigenze clinico/assistenziali che per l'eterogeneità delle tecnologie utilizzate.

D'altra parte, la natura stessa del processo di prevenzione, cura ed assistenza, che richiede la partecipazione di più competenze e strutture professionali e l'evoluzione del sistema sanitario sempre più verso modelli a rete basati sulla collaborazione sul territorio, rende necessaria -ancor più che in altri settori- la definizione di regole comuni che consentano tale collaborazione, nell'interesse del singolo cittadino e del servizio sanitario nel suo complesso.

Secondariamente a questa finalità principale non vanno trascurate le esigenze normative finalizzate al supporto a decisioni di politica sanitaria da parte delle Istituzioni oltre alle attività di ricerca medica, sempre più significative e rilevanti ai fini della salute del cittadino.

Tenendo conto di queste peculiarità, obiettivo di questo questo documento è definire un codice di condotta per la protezione dei dati personali di validità generale, che definisca regole comuni, applicabili nelle diverse strutture indipendentemente dalle singole caratteristiche organizzative e tecnologiche.

Nel primo capitolo viene definito un modello di riferimento -indipendente dagli specifici contesti organizzativi e tecnologici- delle varie tipologie di trattamento implementabili nelle organizzazioni sanitarie, in termini di processi sottostanti con le relative attività, profili professionali coinvolti e tipologia dati personali necessari.

Sulla base di questo modello, nei capitoli successivi vengono definite le regole proposte dal Codice in relazione ai principi ed agli obblighi ("accountability") definiti dal Regolamento, come schematizzati in figura


Le regole esprimono in modo esaustivo e non ambiguo le misure tecnico-organizzative da adottare e sono correlate con i relativi fondamenti giuridici, sia relativamente al Regolamento che alle altre normative applicabili.

Stante la rilevanza dei dati personali in tutta la struttura organizzativa, per la natura stessa dei processi eseguiti e dei servizi erogati, la definizione delle regole è articolata in due sezioni:

- la prima relativa alla definizione di regole di validità generale, di rilevanza per l'intera organizzazione del titolare;
- la seconda relativa alle regole specifiche applicabili nelle diverse tipologie di trattamento:

Conformemente alla struttura del Regolamento, le regole sono a loro volta articolate in due gruppi:

- regole relative ad obblighi in termini di diritti e misure nei confronti dell'interessato;
- regole relative ad obblighi in termini di misure organizzative interne necessarie

## Indice

# 1. Modello di riferimento dei trattamenti nelle organizzazioni sanitarie

## 1.1 Premessa

Le strutture e le esigenze delle organizzazioni sanitarie sono molteplici, sia per la varietà dei contesti organizzativi (individuali, locali, territoriali), sia per la molteplicità delle patologie e forme assistenziali, ognuna delle quali con possibili requisiti specifici, sia per la varietà delle stesse che per l'eterogeneità delle tecnologie utilizzate.

In questo "Capitolo 1" -avente solo valore informativo ai fini del codice- viene definito un modello di riferimento di validità generale -indipendente dai singoli contesti- dei processi eseguiti nelle organizzazioni sanitarie in relazione alle esigenze di trattamento dei dati personali, evidenziando le tipologie di dati gestiti, le figure professionali coinvolte e le specifiche esigenze a fronte delle singole attività, con l'obiettivo di individuare -innanzi tutto- le finalità e la liceità dei trattamenti effettuati.

Approfondendo e dettagliando questo modello secondo le prospettive ed i principi del Regolamento nei successivi capitoli sono definiti gli aspetti normativi del codice, con le regole applicabili per le diverse aree di "accountability", sempre secondo un approccio indipendente da specifiche soluzioni organizzative ed implementative.

## 1.2 Definizioni

**Contatto** [1]

Si definisce **"contatto"** l'incontro e/o la comunicazione tra un paziente e una struttura o un professionista sanitario in relazione ad una esigenza sanitaria del paziente stesso, indipendentemente dal numero di prestazioni erogate durante il contatto.
Il contatto può attuarsi in un singolo momento puntuale (comunicazione o incontro) o evolversi per un periodo di tempo (es. degenza).
Nel caso in cui un contatto si protragga in più incontri (per esempio un ciclo di terapia) si considera come un unico contatto.

**Percorso di cura** [1]

Si definisce **"percorso"** una serie di contatti tra un paziente e una o più strutture sanitarie e/o singoli professionisti per uno specifico problema di

[1] cfr: *http://www.mattoni.salute.gov.it/mattoni/documenti/M5_Standard_Milestone_1.6.pdf*

salute che inizia con la diagnosi e termina con una soluzione, anche se non definitiva, del problema.

**Atto sanitario** [1]

Si definisce "**atto sanitario**" qualsiasi attività, rivolta al singolo individuo, a gruppi o alla collettività, di prevenzione, analisi del rischio (valutazione, gestione e comunicazione), nonché di prescrizione connessa alla salute ed alla sicurezza negli ambienti di vita e di lavoro; attività di diagnosi, cura e assistenza di qualsiasi condizione modificante lo stato di salute della Persona ed in condizioni di comprovata disabilità, nella prospettiva tracciata dalla Classificazione Internazionale del Funzionamento, secondo le indicazioni dell'OMS; qualsiasi attività volta alla prevenzione, educazione e formazione alla salute, valutazione, cura, assistenza di qualsiasi condizione, anche con l'utilizzo di tecnologie avanzate di supporto alle funzioni vitali e con la collaborazione di personale di supporto, palliazione, abilitazione, riabilitazione e rieducazione di alterazioni strutturali o funzionali, anche con l'ausilio di dispositivi medici, che comportino limitazioni delle attività e/o restrizioni della partecipazione sociale relative a qualsiasi condizione psicofisica di vita della Persona stessa, nel suo ambiente naturale e sociale.

**Nucleo di Riferimento**

Si definisce "**Nucleo di Riferimento**" una Unità Operativa o un gruppo di professionisti o un singolo professionista all'interno della organizzazione del titolare che -nell'ambito di un contatto e per un certo periodo di tempo- ha la responsabilità di gestire e coordinare i servizi per l'interessato, effettuando direttamente e/o richiedendo le prestazioni necessarie ad altre Unità Operative della struttura e/o ad altre strutture (anche in qualità di fornitori di servizi esternalizzati) e/o a singoli professionisti interni o esterni alla struttura del titolare.

**Processo**

Si definisce "**processo**" un insieme di attività ("atti sanitari", attività organizzative, attività amministrative e attività logistiche) sinergiche e strumentali all'erogazione dei servizi oggetto del trattamento

**Regolamento**

Per semplicità espressiva, nel seguito di questo documento, con "**Regolamento**" si intende il combinato di quanto prescritto dal Regolamento UE 2016/679 e dal Dlgs 101/2018 di adeguamento della normativa nazionale.

[1] CONAPS – Coordinamento nazionale associazioni professioni sanitarie – www.conaps.it

**Dati personali**

Per semplicità espressiva, nel seguito di questo documento, con "**dati personali**" si individuano genericamente tutti i dati personali gestiti e raccolti dal titolare, che includono anche quei dati relativi alla salute dell'interessato e quei dati idonei a rivelare lo stato di salute dell'interessato, come definiti nel § 4.15 del Regolamento.

## 1.3 Trattamenti e finalità

Il trattamento di dati personali all'interno di una organizzazione sanitaria (titolare) è finalizzato alla erogazione all'interessato -nel modo più sicuro, economico ed efficiente- dei servizi sanitari, socio-sanitari e socio-assistenziali appropriati e di qualità, intesi genericamente come servizi di profilassi, di diagnosi, di cura e di assistenza, necessari a far fronte ad una specifica esigenza sanitaria nell'interesse della persona richiedente.

L'interessato -o in sua vece altri soggetti legittimati- chiede espressamente l'erogazione dei servizi sanitari alla organizzazione ("erogazione in elezione"), ovvero l'organizzazione eroga i servizi sanitari in una situazione di emergenza ("erogazione in urgenza"), per la salvaguardia degli interessi di salute dell'interessato. Sia al momento dell'inizio dell'erogazione del servizio sanitario che durante l'evoluzione dello stesso, l'interessato può presentare -sia per ragioni di età che per il suo stato di salute- condizioni di coscienza e comprensione diverse: dalla completa incoscienza alla piena consapevolezza.

In subordine a questo trattamento, derivante dalla missione dell'organizzazione sanitaria e da obbligo legale del titolare, possono essere implementati dallo stesso titolare ulteriori ed autonomi trattamenti secondari, utili al raggiungimento dell'obiettivo di cura o di assistenza nell'interesse del singolo o della collettività ed al miglioramento dell'organizzazione, finalizzati a:

a) analisi statistiche ed epidemiologiche a scopo di prevenzione, sia a livello di popolazione che di singolo individuo;
b) analisi statistiche ed epidemiologiche a supporto di decisioni di politica sanitaria a fronte di requisiti normativi;
c) analisi finalizzate al supporto di decisioni del titolare in merito alla organizzazione della propria struttura e della propria offerta di servizi;
d) ricerca in campo medico;
e) implementazione, gestione e manutenzione dell'infrastruttura tecnologica.

## 1.3 Tipologie di dati gestiti e raccolti

I dati personali raccolti e gestiti dal titolare riguardano informazioni di diversa natura (dati anagrafici, demografici, stili di vita, etc.) inclusi dati relativi alla salute dell'interessato e dati idonei a rivelare lo stato di salute dell'interessato, come definiti nel § 4.15 del Regolamento:

a) forniti autonomamente dall'interessato stesso;
b) forniti da familiari, care-giver ed altre figure giuridiche di riferimento;
c) raccolti ed elaborati durante il processo di cura ed assistenziale da parte del titolare;
d) trasmessi da altre organizzazioni sanitarie che abbiano erogato in passato o eroghino al momento servizi sanitari all'interessato, al fine di consentire una più precisa e sicura valutazione dello stato di salute dell'interessato stesso e dell'appropriatezza e sicurezza dei servizi da erogare.

## 1.4 Trattamento di dati personali finalizzato all'erogazione dei servizi sanitari all'interessato

### 1.4.1 Scenario complessivo

L'erogazione di servizi sanitari si articola in un insieme di **processi** eseguiti dal titolare nell'ambito di singoli **contatti** -e/o di più contatti separati ma consequenziali per costituire un percorso- per scopi preventivi, profilattici, diagnostici, terapeutici e assistenziali. Ogni processo si articola in **atti sanitari** ed in attività organizzative, amministrative e logistiche sinergiche e strumentali all'erogazione dei servizi.

Nell'ambito del contatto all'interno della struttura del titolare, dal punto di vista clinico ed organizzativo, un **Nucleo di Riferimento** ha la responsabilità di gestire i servizi per l'interessato, effettuando direttamente e/o richiedendo e coordinando le prestazioni necessarie ad altre Unità Operative della struttura e/o ad altre strutture e/o a singoli professionisti.

L'erogazione di questi servizi può anche richiedere -sia durante il contatto che prima e dopo il contatto stesso, senza limiti di tempo- la collaborazione e la conseguente condivisione di dati personali dell'interessato con altri operatori sanitari sul territorio -singoli soggetti e/o strutture-

a) per acquisire e/o fornire informazioni sullo stato di salute dell'interessato stesso, utili ai fini della sicurezza ed appropriatezza del servizio sanitario erogato da parte del titolare e/o l'erogazione di

servizi sanitari da parte di altri titolari (es. il medico curante, specialisti, etc. che seguono l'interessato);

b) per scopi di consulenza su aspetti specifici;

c) per l'attuazione di percorsi diagnostici, terapeutici ed assistenziali che si estendono nel tempo e sul territorio, quali patologie croniche e/o situazioni sanitarie che richiedono attività di assistenza e di cura correlate e sinergiche, eseguite da professionalità e strutture diverse tramite contatti indipendenti e temporalmente/localmente circoscritti.
*Nota:*
*In questo scenario, Nuclei di Riferimento di diverse strutture collaborano -ognuno per le aree di propria responsabilità- condividendo i dati dell'interessato per costituire un unico Nucleo di Riferimento complessivo del percorso diagnostico-terapeutico-assistenziale .*

### 1.4.2 Attività che comportano l'accesso ai dati personali e dati necessari

Nell'ambito dell'insieme dei processi implementati nella organizzazione del titolare per l'erogazione dei servizi sanitari all'interessato, le attività che richiedono l'utilizzo dei dati personali sono classificabili in quattro categorie:

1. La valutazione delle esigenze e l'effettuazione di atti sanitari, in presenza o in assenza[1] dell'interessato, da parte di personale medico e/o assistenziale della organizzazione del titolare coinvolto nella cura/assistenza dell'interessato e/o di professionisti esterni consultati per scopi di consulenza su aspetti specifici inerenti la salute dell'interessato stesso, anche mediante la richiesta di dati ad altri titolari che abbiano -in precedenza senza limiti di tempo- erogato servizi sanitari all'interessato.

2. La comunicazione di dati personali ad altri titolari che abbiano al momento in cura e/o assistenza l'interessato e che facciano richiesta di informazioni per valutarne lo stato di salute e definire con maggiore appropriatezza i servizi sanitari da erogare all'interessato stesso.

3. La programmazione e l'organizzazione delle risorse e delle attività all'interno della struttura, effettuata da parte di personale sanitario

[1] ad esempio nei casi di telemedicina, di tele-monitoraggio o di richiesta di supporto telefonico da parte dell'interessato stesso

e/o amministrativo, ai fini dell'efficacia, dell'efficienza e della sicurezza dei servizi erogati;

4. L'espletamento di attività amministrative (quali -ad esempio- la rendicontazione nei confronti di Istituzioni, la fatturazione verso l'interessato e/o verso terzi, l'archiviazione della documentazione e la produzione di copie su richiesta dell'interessato) a fronte dei servizi erogati;

Tutte le attività di cui ai punti precedenti possono essere condotte da personale dell'organizzazione del titolare o da personale di strutture esterne alle quali il titolare abbia affidato -mediante un apposito contratto- la responsabilità delle specifiche attività.

Le attività sono condotte sia mediante strumenti tecnologici che con metodi manuali (cartacei), secondo procedure e metodi diversi dipendenti dall'organizzazione dei singoli titolari.

**Esempi**

A titolo esemplificativo, senza pretesa di completezza, si elencano nel seguito alcune delle attività più frequenti che rientrano nei gruppi citati

**Valutazione delle esigenze ed effettuazione di atti sanitari**

- Interazioni con il paziente prima o dopo il contatto per acquisire informazioni sul suo stato di salute ai fini di valutare al meglio le necessità
- Richieste di consulenze mediche esterne ed esami diagnostici
- Prestazioni di consulenze mediche, pre-ricovero chirurgiche e visite di controllo
- Prestazioni specialistiche ambulatoriali, specialistiche, riabilitative
- Anamnesi, refertazione e dimissione pazienti
- Definizione di percorsi diagnostici, terapeutici e riabilitativi
- Analisi e gestione della qualità, comprese indagini di gradimento
- Prestazioni domiciliari
- Assistenza infermieristica e/o somministrazione di farmaci e terapie
- Assistenza alla persona
- Attività di affiancamento, formazione e tutoraggio tirocinanti
- Valutazione di eventi clinici pregressi

**Programmazione di risorse ed attività**

- Gestione delle liste di attesa
- Gestione delle liste operatorie
- Gestione delle liste di lavoro delle singole UO
- Ordine/acquisizione di farmaci e dispositivi medici
- Accettazione al ricovero
- Interazione con il paziente prima o dopo il contatto per definire aspetti organizzativi e logistici del servizio

**Attività amministrative a fronte dei servizi erogati**

- Controlli codifiche SDO e controlli di merito-completezza delle cartelle cliniche
- Invio flussi e rendicontazione di prestazioni socio-sanitarie
- Invio flussi di ricovero e prestazioni ambulatoriali
- Fatturazioni verso SSN, l'interessato o terzi pagatori
- Relazioni con il pubblico e gestione di segnalazioni di reclami ed encomi
- Gestione sinistri e richieste di risarcimento
- Prenotazione ed accettazione /gestione ingressi di prestazioni, di ricovero, ambulatoriali e RSA
- Fatturazione ticket e assicurazioni e gestione incassi
- Archiviazione e gestione registri, fascicoli e documentazione sanitaria
- Interazione con il paziente prima o dopo il contatto in merito agli aspetti amministrativi inerenti al servizio da erogare o erogato
- Rappresentazione dell'organizzazione in giudizio inerenti l'erogazione di servizi sanitari
- Gestione pratiche legali ed istituzionali inerenti l'erogazione di servizi sanitari con conseguente de-archiviazione di dati personali

### 1.4.3 Necessità e criteri circa l'accesso ai dati personali

Relativamente alle tipologie di attività che richiedono l'accesso ai dati personali si individuano le necessità di accesso come descritto nel seguito.

#### 1.4.3.1 Tipologie di dati necessari

1. Valutazione delle esigenze ed effettuazione di atti sanitari
   Per la sicurezza e l'efficacia di queste attività, è necessario che il personale medico ed assistenziale interessato abbia accesso

a tutte le informazioni disponibili sull'interessato, presenti e pregresse, alcune delle quali -dipendenti dall'attività in corso- assolutamente necessarie, le altre comunque utili per rappresentare il quadro completo dello stato di salute della persona aumentando quindi la sicurezza dell'atto sanitario.

Nell'attuazione delle singole prestazioni è possibile che collabori anche personale tecnico specializzato, che può avere necessità di accedere a specifiche informazioni personali, la cui tipologia dipende dalla natura della prestazione effettuata.

2. Comunicazione di dati personali ad altri titolari che ne facciano legittimamente richiesta
   Per l'effettuazione di questa attività è necessario avere accesso all'insieme dei dati personali dell'interessato, per individuare e trasmettere quelli richiesti.

3. Programmazione ed organizzazione delle risorse e delle attività
   Per l'effettuazione di questa attività è necessario avere accesso a specifici dati personali, dipendenti dalla natura del processo effettuato.

4. Attività amministrative a fronte dei servizi erogati
   Per l'espletamento di tali attività è necessario avere accesso ai dati personali:
   1. previsti dalle normative, in caso di rendicontazione alle Istituzioni;
   2. previsti dal contratto stipulato dall'interessato nel caso di fatturazione.

### 1.4.3.2 Abilitazione all'accesso all'interno dell'organizzazione

a) Il personale del "centro di riferimento" responsabile del coordinamento dei servizi sanitari ha accesso -secondo i criteri esposti nel § 1.4.3.1.a- ai dati personali dei soli pazienti di cui ha la responsabilità e per la sola durata del contatto.

b) I destinatari delle richieste di prestazioni per un interessato (singoli individui o personale della Unità Organizzativa),

hanno accesso -secondo i criteri esposti nel § 2.3.1.a- ai dati personali dei soli pazienti per i quali fornisce la prestazione e per la sola durata del contatto.

c) Il personale preposto ai processi di programmazione ed organizzazione delle risorse e delle attività ha accesso -secondo i criteri esposti nel §2.3.1.b- ai dati personali di tutti i pazienti per i quali, al momento è in corso o è previsto un contatto.

d) Il personale preposto alle attività amministrative ha accesso -secondo i criteri esposti nel §2.3.1.c- ai dati personali di tutti i pazienti per i quali, al momento è in corso o è previsto un contatto.

### 1.4.4 Esigenze particolari

a) Il personale medico facente parte del "centro di riferimento" avente la responsabilità paziente può non essere disponibile con continuità (ad esempio in caso di turnazioni notturne, giorni festivi, situazioni prioritarie di emergenza).

Per far fronte a tali casi, l'organizzazione prevede comunque la presenza di figure professionali adeguate in grado di intervenire in caso di necessità a supporto di tutta la struttura.

Il ruolo, in questa veste, di tali professionisti è circoscritto a periodi di tempo definiti e formalizzato con atti ufficiali da parte del titolare.

*Nota:*
*esempio tipico nel contesto ospedaliero è la figura del "medico di guardia", in organizzazioni più ridotte, quali ambulatori e studi professionali la figura del "sostituto".*

Tale ruolo e responsabilità, è individualmente definito, è circoscritto a periodi di tempo definiti e formalizzato con atti ufficiali dei relativi responsabili dell'organizzazione.

In tali situazioni, e per il solo periodo di tempo di responsabilità, questi professionisti hanno necessità di accedere, secondo i criteri esposti nel § 2.3.1.a, a tutte le informazioni del singolo interessato per il quale è necessario un atto sanitario.

b) Accesso alle informazioni al di fuori di un contatto, a fronte di una richiesta da parte dell'interessato e/o di un altro operatore sanitario che ha al momento in cura il paziente.

In qualsiasi momento -senza limiti temporali- il titolare può ricevere da altri titolari, strutture o singoli professionisti al momento impegnati nell'erogazione di servizi sanitari all'interessato, la richiesta di dati personali raccolti dal titolare durante l'erogazione di servizi sanitari erogati in precedenza all'interessato, utili per valutare lo stato di salute dell'interessato ed assicurare la sicurezza e l'appropriatezza del servizio sanitario erogato.

## 1.5 Trattamenti relativi ad analisi statistiche ed epidemiologiche finalizzate alla prevenzione, sia a livello di popolazione che di singolo individuo

### 1.5.1 Scenario

A fronte di esigenze contingenti e/o nell'ambito di protocolli clinici consolidati e/o a seguito delle risultanze di nuove attività di ricerca, il titolare può implementare trattamenti specifici di natura statistica ed epidemiologica, finalizzati a scopi di prevenzione, sia nell'ottica di iniziative di interesse per la salute collettiva che relativamente ai singoli potenzialmente interessati.

Ogni trattamento ha una propria specifica finalità, espressamente definita.

### 1.5.2 Necessità e criteri circa l'accesso ai dati personali

#### 1.5.2.1 Tipologie di dati necessari

Questi trattamenti sono eseguiti con strumenti informatici, e -salvo casi particolari- aumentano di validità e di affidabilità mediante l'accesso a e l'analisi di tutti i dati personali disponibili al titolare, sia quelli anagrafici ed epidemiologici che quelli specifici sulla salute.

Per l'effettuazione di tali analisi non sono necessari dati che consentano (direttamente o mediante semplice derivazione) l'identificazione degli interessati, ma è sufficiente poter collegare

i dati a generici soggetti anonimi, purché sia garantita l'unicità del soggetto (anonimo) al quale si riferiscono i dati stessi.

Deve altresì essere possibile, qualora l'analisi riveli situazioni di rischio, risalire all'identità degli interessati, in modo da poterli informare ed eseguire quanto necessario, nell'interesse degli stessi e della collettività.

#### 1.5.2.2 Abilitazione all'accesso all'interno dell'organizzazione

I ricercatori -personale tecnico e sanitario- responsabili delle analisi hanno accesso a tutte le informazioni disponibili (che escludono -si ripete- dati che consentano l'individuazione degli interessati).

L'identificazione dei singoli interessati, evidenziati dal trattamento come soggetti necessari di servizi sanitari a scopo di prevenzione e/o cura, viene effettuata da personale appositamente ed individualmente autorizzato.

## 1.6 Trattamenti relativi ad analisi statistiche ed epidemiologiche finalizzate a decisioni di politica sanitaria, obbligatori a fronte di requisiti normativi

### 1.6.1 Scenario

A fronte di requisiti normativi il titolare ha l'obbligo di implementare trattamenti per l'analisi e/o il trasferimento di dati personali -anche identificativi dell'interessato- a favore di Enti ed Istituzioni locali, regionali, statali.

Ogni trattamento ha una propria specifica finalità, espressamente definita.

### 1.6.2 Necessità e criteri circa l'accesso ai dati personali

#### 1.6.2.1 Tipologie di dati necessari

I dati necessari nei trattamenti comprendenti dati personali (anche identificativi dell'interessato) ed obbligatoriamente implementati dal titolare per rispondere a requisiti normativi sono definiti nelle normative stesse.

#### 1.6.2.2 Abilitazione all'accesso all'interno dell'organizzazione

Il personale preposto ai trattamenti comprendenti dati personali anche identificativi dell'interessato ed obbligatoriamente implementati dal titolare per rispondere a requisiti normativi è individualmente e specificatamente autorizzato.

## 1.7 Trattamenti finalizzati ad analisi a supporto di decisioni del titolare in merito alla propria attività

### 1.7.1 Scenario

Il titolare può autonomamente implementare trattamenti finalizzati a ottenere informazioni sulle caratteristiche cliniche ed epidemiologiche sul proprio bacino di utenza per ottimizzare la propria organizzazione e la propria offerta di servizi sanitari

Questi trattamenti sono classificabili in due categorie :

a) trattamenti basati su dati anonimi, finalizzati all'analisi dell'utenza, dei servizi erogati e delle attività espletate, a fini di decisioni organizzative interne

b) trattamenti finalizzati alla interazione con i singoli interessati per scopi di fidelizzazione e presentazione/promozione di servizi

Ogni trattamento ha una propria specifica finalità, espressamente definita.

### 1.7.2 Necessità e criteri circa l'accesso ai dati personali

#### 1.7.2.1 Tipologie di dati necessari

a) trattamenti basati su dati anonimi, finalizzati all'analisi dell'utenza, dei servizi erogati e delle attività espletate, a fini di decisioni organizzative interne

I trattamenti implementati dal titolare per analizzare e migliorare la propria organizzazione e la propria offerta di servizi sanitari possono basarsi anche sull'utilizzo di dati personali, resi comunque del tutto anonimi. Non richiedono

l'accesso ad informazioni che consentano (direttamente o mediante semplice derivazione) l'identificazione degli interessati. E' sufficiente poter collegare fra loro tutti i dati rispondenti allo stessa persona, che può quindi essere classificata tramite un codice anonimo, che non consenta di identificare in alcun modo il singolo interessato.

b) trattamenti finalizzati alla interazione con i singoli interessati per scopi di fidelizzazione e presentazione/promozione di servizi

I trattamenti implementati dal titolare finalizzati alla interazione con singoli e/o gruppi di interessati per scopi di fidelizzazione e presentazione/promozione di servizi richiedono l'accesso ai dati identificativi dell'interessato e, a seconda delle finalità, ad alcuni specifici dati personali relativi allo stato di salute.

#### 1.7.2.2 Abilitazione all'accesso all'interno dell'organizzazione

a) trattamenti basati su dati anonimi, finalizzati all'analisi dell'utenza, dei servizi erogati e delle attività espletate, a fini di decisioni organizzative interne

In quanto basati esclusivamente su dati anonimi non sono necessarie autorizzazioni specifiche, in aggiunta a quanto in essere nell'organizzazione per l'identificazione e l'abilitazione degli utenti all'accesso al sistema informativo.

b) trattamenti finalizzati alla interazione con i singoli interessati per scopi di fidelizzazione e presentazione/promozione di servizi

Per i trattamenti che comportano l'identificazione delle persone e l'eventuale accesso a dati personali sono eseguiti da personale esplicitamente ed appositamente autorizzato.

## 1.8 Trattamenti finalizzati alla ricerca in campo medico.

### 1.8.1 Scenario

Le attività di ricerca in campo medico possono articolarsi secondo due scenari:

a) erogazione di servizi ed effettuazione di atti sanitari particolari (sperimentali e non) a specifici pazienti nel corso di un percorso sanitario al fine di valutarne l'efficacia;
b) effettuazione di analisi massive su tutti i dati disponibili di più pazienti al fine di verificare e/o individuare correlazioni fra i dati stessi e derivare informazioni utili dal punto di vista medico.

Ogni trattamento ha una propria specifica finalità, espressamente definita.

### 1.8.2 Necessità e criteri circa l'accesso ai dati personali

#### 1.8.2.1 Tipologie di dati necessari

a) Erogazione di servizi ed effettuazione di atti sanitari particolari (sperimentali e non) a specifici pazienti nel corso di un percorso sanitario, al fine di valutarne l'efficacia.

L'effettuazione di queste attività rientra all'interno del trattamento finalizzato all'erogazione di servizi sanitari, di cui al § 1.4, nell'ambito del quale sono anche valutati i risultati ottenuti sulla specifica persona. Richiedono quindi l'accesso ai dati personali secondo i criteri descritti al § 1.4.2.1.

La eventuale valutazione di queste attività su insiemi più ampi di persone rientra nel caso di analisi massive, di cui al seguente punto b).

b) Effettuazione di analisi massive su tutti i dati disponibili di più pazienti al fine di verificare e/o individuare correlazioni fra i dati stessi e derivare informazioni utili dal punto di vista medico.

Questi trattamenti sono eseguiti con strumenti informatici, e - salvo casi particolari- aumentano di validità e di affidabilità mediante l'accesso a e l'analisi di tutti i dati personali disponibili al titolare, sia quelli anagrafici ed epidemiologici che quelli specifici sulla salute.

Per l'effettuazione di tali analisi non sono necessari dati che consentano (direttamente o mediante semplice derivazione) l'identificazione degli interessati, ma è sufficiente poter collegare i dati a generici soggetti anonimi, purché sia garantita l'unicità del soggetto (anonimo) al quale si riferiscono i dati stessi.

Deve altresì essere possibile, qualora l'analisi riveli situazioni di rischio o comunque rilevanti per la persona, risalire all'identità degli interessati, in modo da poterli informare ed eseguire quanto necessario, nell'interesse degli stessi e della collettività.

#### 1.8.2.2 Abilitazione all'accesso all'interno dell'organizzazione

a) Erogazione di servizi ed effettuazione di atti sanitari particolari (sperimentali e non) a specifici pazienti nel corso di un percorso sanitario, al fine di valutarne l'efficacia.

   L'effettuazione di queste attività rientra all'interno del trattamento finalizzato all'erogazione di servizi sanitari, di cui al § 1.4. Si applicano quindi i criteri di abilitazione descritti al § 1.4.2.2

b) Effettuazione di analisi massive su tutti i dati disponibili di più pazienti al fine di verificare e/o individuare correlazioni fra i dati stessi e derivare informazioni utili dal punto di vista medico.

   I ricercatori -personale tecnico e sanitario- responsabili delle analisi hanno accesso a tutte le informazioni disponibili (che escludono -si ripete- dati che consentano l'individuazione degli interessati).

   L'identificazione dei singoli interessati, evidenziati dal trattamento come soggetti di specifico interesse con i quali comunicare per ulteriori informazioni e/o erogazione di ulteriori servizi sanitari, viene effettuata da personale appositamente ed individualmente autorizzato.

## 1.9 Trattamenti finalizzati alla gestione della infrastruttura tecnologica

### 1.9.1 Scenario complessivo

L'infrastruttura tecnologica implementata dall'organizzazione -localmente e/o in cloud- a supporto delle varie attività può comprendere

procedure software, archivi, dispositivi -medici e non- e strumenti di comunicazione che acquisiscono, trasmettono e registrano anche (ma non solo) dati personali.

Le relative attività di implementazione, gestione, manutenzione sono eseguite -localmente o in cloud- da personale dell'organizzazione del titolare o da personale di strutture esterne alle quali il titolare abbia affidato -mediante un apposito contratto- la responsabilità delle specifiche attività.

### 1.9.2 Necessità e criteri circa l'accesso ai dati personali

#### 1.9.2.1 Tipologie di dati necessari

Nell'ambito dei processi implementati dal titolare per la implementazione, gestione e manutenzione dell'infrastruttura tecnologica hanno necessità di accesso ai dati personali

a) le attività di back-office, eseguite per la rettifica -direttamente negli archivi informatizzati- di errori materiali commessi in fase di inserimento dati nel sistema informativo o derivanti da malfunzionamenti delle procedure informatiche.

b) le attività di gestione e manutenzione effettuate su dispositivi ed apparecchiature che -per limitazione tecnologica- non consentano la definizione di premessi di abilitazione diversificati all'esecuzione delle diverse attività.

Altre attività inerenti all'implementazione, alla gestione ed alla manutenzione dell'infrastruttura tecnologica non hanno necessità di accesso ai dati personali.

#### 1.9.2.2 Abilitazione all'accesso all'interno dell'organizzazione

Il personale preposto ai trattamenti che comportino -direttamente (caso 1.9.2.1a) o indirettamente (caso 1.9.2.1.b)- l'accesso ai dati personali dell'interessato ha accesso a tutte le informazioni personali registrate nel sistema secondo opportune regole di abilitazione e nel rispetto di meccanismi di tracciamento delle attività effettuate.

**Capitoli successivi da dettagliare**

2. Regole di validità generale per l'intera organizzazione del titolare
   - 2.1 Regole relative ad obblighi verso l'interessato
   - 2.2 Regole relative ad obblighi in termini di misure organizzative interne

3. Regole specifiche per le singole tipologie di trattamento

3.1 Trattamento di dati personali finalizzato all'erogazione dei servizi sanitari all'interessato
   - 3.1.1 Regole relative ad obblighi verso l'interessato
   - 3.1.2 Regole relative ad obblighi in termini di misure organizzative interne

3.2 Trattamenti relativi ad analisi statistiche ed epidemiologiche finalizzate alla prevenzione, sia a livello di popolazione che di singolo individuo
   - 3.2.1 Regole relative ad obblighi verso l'interessato
   - 3.2.2 Regole relative ad obblighi in termini di misure organizzative interne

3.3 Trattamenti relativi ad analisi statistiche ed epidemiologiche finalizzate a decisioni di politica sanitaria, obbligatori a fronte di requisiti normativi
   - 3.3.1 Regole relative ad obblighi verso l'interessato
   - 3.3.2 Regole relative ad obblighi in termini di misure organizzative interne

3.4 Trattamenti relativi ad analisi statistiche ed epidemiologiche finalizzate al supporto a decisioni del titolare in merito alla propria struttura
   - 3.4.1 Regole relative ad obblighi verso l'interessato
   - 3.4.2 Regole relative ad obblighi in termini di misure organizzative interne

3.5 Trattamenti finalizzati alla ricerca in campo medico
   - 3.5.1 Regole relative ad obblighi verso l'interessato
   - 3.5.2 Regole relative ad obblighi in termini di misure organizzative interne

3.6 Trattamenti finalizzati alla implementazione, gestione e manutenzione dell'infrastruttura tecnologica
   - 3.6.1 Regole relative ad obblighi verso l'interessato
   - 3.6.2 Regole relative ad obblighi in termini di misure organizzative interne