Codice di condotta per la protezione dei dati personali in sanità

Sulla base del modello dei trattamenti definito alla fine dello scorso anno (doc. fmf-174/1018 ver 1.0 del 11.11.2018) e di contributi forniti dai vari partecipanti per i vari ambiti di accountability previsti dal Regolamento, questo documento costituisce una prima bozza del possibile Codice di condotta.

In questa fase ci si è concentrati principalmente sulla individuazione delle caratteristiche e dei requisiti peculiari del contesto sanitario e sulla conseguente individuazione di regole, indipendenti da specifici contesti organizzativi e tecnologici, tali da permettere il rispetto degli obblighi previsti dal Regolamento.

Successivamente al consolidamento di un tale quadro di riferimento complessivo in termini di requisiti e di regole, i singoli aspetti saranno ove necessario raffinati e corredati degli opportuni riferimenti giuridici rispetto alle normative di rilevanza.

*Tutti i partecipanti all'iniziativa sono invitati ad esprimere il loro consenso ed a fornire il loro contributo sulle varie sezioni di questo documento -anche in termini di identificazione di ulteriori aree di approfondimento da affrontare successivamente- **entro il 15 marzo 2019**, mediante la compilazione dell'apposito modulo (doc. fmf-018/0219) presente sul sito.*

Codice documento	fmf-001/0119
Data	22-02-2019
Versione	0.91

Indice

1. Premessa

1.1 Obiettivo e struttura del codice di condotta

Il presente codice di condotta definisce criteri e regole secondo cui declinare gli obblighi previsti dal Regolamento UE 2016/679 all'interno di una organizzazione sanitaria, che eroghi servizi sanitari autonomamente o in collaborazione con altre organizzazioni sanitarie sul territorio nell'interesse dell'assistito.

Come prescritto dall'Articolo 40 del Regolamento[1], un Codice di condotta ha lo scopo di dettagliare criteri e regole, pratiche e misurabili, secondo cui declinare le prescrizioni del Regolamento nello specifico contesto operativo di un determinato settore. Di conseguenza, la struttura di questo documento può essere concettualmente suddivisa in due parti:

a) la descrizione -all' articolo 3- delle caratteristiche e delle peculiarità del contesto sanitario, sotto il profilo dei dati gestiti e delle tipologie di trattamento effettuate, secondo un modello di riferimento di validità generale, indipendente dalle dimensioni dell'organizzazione, dalla sua struttura e dalle soluzioni tecnologiche implementate;

b) la definizione -negli articoli successivi- dei criteri e delle regole da adottare per l'applicazione delle disposizioni del regolamento nell'organizzazione, espresse in una forma non ambigua ma al tempo stesso di validità generale, da attualizzarsi da parte del titolare nel suo specifico contesto organizzativo e tecnologico.

1.2 Approccio

In accordo con quanto prescritto dal Regolamento in merito alla necessità di un approccio complessivo, tecnico ed organizzativo, alla protezione dei dati personali (art. 24), elemento principale e fondante di questo codice di condotta è la istituzione da parte del titolare di un "Sistema di gestione per la protezione dei dati personali", nell'ambito del quale definire, implementare e controllare, in un quadro unitario e coerente, tutti gli aspetti rilevanti la protezione dei dati personali e che possa evolversi nel tempo secondo in un'ottica di continuo miglioramento e di rispondenza ai requisiti dell'organizzazione e a nuove normative.

Considerata l'eterogeneità delle diverse organizzazioni sanitarie in termini di diversità e molteplicità di scenari operativi e di contesti tecnologici all'interno della stessa organizzazione, è verosimile che l'adozione di tutte le indicazioni del

[1] cfr anche linee guida definite il 12.2.2019 da European Data Protecton Board https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf

Codice di condotta da parte di un titolare possa non essere contestuale, ma avvenire gradualmente nel tempo, relativamente a specifici aspetti.

In questa ottica, fra i documenti del "Sistema di gestione per la protezione dei dati personali" è previsto un documento che espliciti le sezioni del codice di condotta al quale il titolare aderisce al momento.

Anche dal punto di vista delle tecnologie, il contesto sanitario è fortemente caratterizzato dalla presenza -nella stessa organizzazione- di molteplici sistemi, applicazioni e dispositivi, -basati su tecnologie diverse e provenienti da fornitori diversi- variamente interconnessi per supportare le varie esigenze.

Questa articolazione fa sì che non sempre sia possibile e/o rapido l'aggiornamento di tutti i sistemi informatizzati (intendendo con questo termine anche i dispositivi medici) per ottenere un ambiente omogeneo rispetto alle funzionalità ed ai livelli di protezione dei dati richiesti.

A questo scopo, per descrivere con chiarezza la situazione in essere e disporre di un quadro di riferimento per valutare i rischi e definire piani evolutivi, il "Sistema per la protezione dei dati personali" prevede la gestione di un documento denominato "Registro dei sistemi informatici", che evidenzi le caratteristiche dei singoli sistemi dal punto di vista della rispondenza a quanto previsto dal codice, con -in caso negativo- la definizione delle misure correttive e degli eventuali piani evolutivi.

1.3 Ambiti

Nella presente versione, il codice è focalizzato a dettagliare criteri e regole relativamente ad un sottoinsieme delle aree di accountability previste dal Regolamento, ritenute di maggiore rilevanza ed urgenza anche per le implicazioni di natura organizzativa ed attuativa.

Per gli altri aspetti, non esplicitamente dettagliati e che saranno oggetto di approfondimento in versioni successive del codice, è previsto che il titolare formalizzi autonomamente delle procedure apposite nell'ambito del Sistema di gestione per la protezione dei dati personali.

2 Definizioni

Regolamento

Per semplicità espressiva, nel seguito di questo documento, con "**Regolamento**" si intende il Regolamento UE 2016/679 e con "**Codice privacy**" si intende il D.Lgs. 196/2003 come modificato dal Dlgs 101/2018 di adeguamento della normativa nazionale. Gli altri atti o provvedimenti nazionali o comunitari sono richiamati di volta in volta con la loro specifica definizione.

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.

Trattamento, Titolare del trattamento, Responsabile del trattamento

Con questi termini si fa riferimento a quanto definito per i corrispondenti termini del § 4 "Definizioni" del Regolamento.

Per semplicità espressiva, con il termine "titolare" si individua il "titolare del trattamento"; con il termine "responsabile" si individua il "responsabile del trattamento"

Contatto

Si definisce **"contatto"** [2] 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 presso la sede dell'organizzazione o del professionista sanitario ovvero presso il domicilio dell'interessato, 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 e/o comunicazioni (per esempio un ciclo di terapia) si considera come un unico contatto.

Percorso

Si definisce **"percorso"** [1, 3] (diagnostico, terapeutico, assistenziale) una serie di contatti coordinati e sinergici tra un assistito e una o più strutture sanitarie e/o socio-sanitarie e/o singoli professionisti a livello ospedaliero e/o territoriale per uno specifico problema di salute che inizia con la diagnosi e termina con una soluzione, anche se non definitiva, del problema. Durante il percorso le diverse strutture ed i diversi professionisti collaborano ed interagiscono nella

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

[3] cfr: https://www.fiaso.it/Questionari/ICT-e-Percorsi-Diagnostico-Terapeutici-Assistenziali-PDTA

valutazione dello stato di salute dell'assistito e nell'organizzazione ed attuazione dei servizi necessari.

Atto sanitario [4]

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/o per un certo periodo di tempo- ha la responsabilità di gestire e coordinare i servizi medici, assistenziali e socio-sanitari 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.

Un Nucleo di Riferimento può operare in collaborazione con altri Nuclei di Riferimento in organizzazioni diverse, che -collegialmente e sinergicamente- assicurano all'interessato i servizi sanitari e socio-sanitari più adatti per le esigenze dell'interessato stesso nell'ambito di un percorso diagnostico terapeutico assistenziale.

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. Le attività costituenti un processo possono essere eseguite, totalmente o parzialmente, mediante il supporto di sistemi informatizzati e/o sulla base di documenti cartacei.

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

Sistema informatizzato

Si definisce "**sistema informatizzato**" l'insieme delle risorse hardware, delle procedure software -di base ed applicative- e dei dispositivi medici, connessi o separati dal resto del sistema informatico, utilizzati per il supporto ad una specifica attività, in collegamento o separatamente rispetto ad altri sistemi.

In relazione alle modalità di uso e di gestione all'interno dell'organizzazione, i sistemi informatizzati sono classificabili in tre categorie:

a. "**centralizzato**", si intendono quei sistemi, usualmente articolati e complessi, di uso diffuso all'interno della struttura, installati per i componenti centrali (server, basi dati, procedure applicative, etc.) in ambienti centralizzati e dedicati e gestiti centralmente da personale dedicato.
b. "**condiviso**", si intendono quei sistemi installati anche nelle componenti centrali all'interno di diversi settori della struttura e utilizzati a supporto specifiche attività sanitarie e/o organizzative di interesse locale per il settore. Operano autonomamente (collegati o meno con il sistema centrale dell'organizzazione) e sono gestiti su chiamata dalla struttura centrale dell'organizzazione e/o da personale dello specifico settore di afferenza.
c. "**individuale**", si intendono quei sistemi, generalmente mobili, utilizzabili individualmente da parte del paziente (all'esterno e/o all'interno del centro) e/o da personale sanitario nell'ambito dell'attività clinica e/o assistenziale.

Salvo esplicita differenziazione nei singoli punti, quanto indicato nel presente codice si applica a tutte le tipologie di sistemi informatizzati.

Mascheramento, pseudonimizzazione

Si definisce "**mascheramento**" dei dati personali il processo di cancellazione di quei dati che consentono l'individuazione della persona o la loro modifica in modo tale che non sia possibile risalire all'identificazione della persona.
Si definisce "**pseudonimizzazione**" il mascheramento dei dati personali, accompagnato dall'associazione agli stessi di un codice crittografato che, una volta decodificato con opportune procedure, fornisca gli elementi per identificare la persona referenziata.

Procedura

Si definisce "**procedura**" un documento che descrive le modalità operative, le risorse e le responsabilità per la gestione e l'esecuzione dei processi o di parte di essi. Se su supporto informatico il documento non deve essere alterabile e deve consentire l'identificazione sicura di colui che la ha approvata e del momento dell'approvazione.

Registrazione

Si definisce "**registrazione**" un documento (su supporto informatico o cartaceo) che riporta i risultati o fornisce evidenza delle attività svolte. Se su supporto informatico il documento non deve essere alterabile.

Riesame

Si definisce "**riesame**" una attività effettuata per riscontrare l'idoneità, l'adeguatezza e l'efficacia dell'oggetto del riesame a conseguire gli obiettivi stabiliti.

Sistema di gestione

Si definisce "**sistema di gestione**" un sistema per stabilire politica ed obiettivi e per conseguire tali obiettivi.

Monitoraggio

Si definisce "**monitoraggio**" l'effettuazione di controlli o misure periodiche condotte su un'attività o un processo al fine di controllarne nel tempo la conformità a regole e criteri predefiniti.

Evidenza

Si definisce "**evidenza**" un insieme di dati e informazioni che supportano l'esistenza o la veridicità di qualcosa

Verifica

Si definisce "**verifica**" la conferma, sostenuta da evidenze oggettive, del soddisfacimento di requisiti specificati.

3. Tipologie di dati, trattamenti e finalità

3.1 Tipologie di dati

3.1.1 Tipologie di dati gestiti e raccolti

I dati personali raccolti e gestiti dal titolare nell'ambito di tutte le tipologie di trattamenti 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) forniti 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.

Il titolare mantiene evidenza dell'origine dei dati raccolti e gestiti, nei sistemi informatizzati se registrati in tali contesti o sui documenti cartacei se gestiti solo in questa forma.

3.1.2 Periodo di conservazione

I dati raccolti sono conservati dal titolare possibilmente senza limiti di tempo, in quanto un quadro il più possibile completo -anche relativamente ad eventi remoti- dello stato di salute del paziente, è necessario per supportare l'affidabilità e la qualità della decisione medica, della diagnosi e del trattamento nell'erogazione dei servizi, nonché la completezza delle analisi di prevenzione, epidemiologiche e statistiche e le attività di ricerca.

In ogni caso, i dati sono conservati per un periodo di tempo minimo:

a) conforme alle disposizioni di legge che definiscono tempi minimi per la conservazione delle varie tipologie di documenti e di registrazioni cliniche;
b) tale da garantire il legittimo interesse del titolare per la tutela dei propri diritti legali e di difesa, in accordo con i termini considerati dalla giurisprudenza corrente [5]

Qualora il titolare venga a conoscenza del decesso dell'interessato, cancella i relativi dati personali dai contesti informatici di supporto alle operatività ordinarie e li conserva secondo i termini e le modalità definite dalle normative di legge applicabili. E' facoltà del titolare rendere anonimi i dati del deceduto, ed utilizzarli per sole finalità epidemiologiche, statistiche e di ricerca.

3.2 Trattamenti

3.2.1 Tipologie di trattamenti

I trattamenti dei dati personali all'interno di una organizzazione sanitaria sono classificabili in cinque categorie, in funzione delle relative finalità:

Trattamento finalizzato all'erogazione dei servizi sanitari, socio-sanitari e socio-assistenziali all'interessato

1. il trattamento principale, derivante dalla missione e dall'obbligo legale dell'organizzazione sanitaria, è l'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 finalizzati alla prevenzione, diagnosi, cura, riabilitazione, palliazione ed assistenza, necessari per far fronte

5 Cfr. Cass. Civ., sez. III, sent. 23/09/2013, n.21715

ad una specifica esigenza sanitaria nell'interesse della persona interessata.
A fronte di e in ottemperanza a specifiche previsioni normative, il titolare ha anche l'obbligo di implementare attività per l'analisi e/o il trasferimento di dati personali -anche identificativi dell'interessato- a favore di Enti ed Istituzioni locali, regionali, statali secondo meccanismi e procedure definite dalle normative stesse.

Trattamenti secondari
In aggiunta a questo trattamento, possono essere implementati dal titolare ulteriori ed autonomi trattamenti, utili al raggiungimento dell'obiettivo di cura o di assistenza nell'interesse del singolo o della collettività ed al miglioramento dell'organizzazione del titolare, classificabili -in funzione della loro finalità in:

2. analisi statistiche ed epidemiologiche a scopo di prevenzione, sia a livello di popolazione che di singolo individuo;
3. analisi finalizzate al supporto di decisioni del titolare in merito alla organizzazione della propria struttura e della propria offerta di servizi;
4. ricerca scientifica;
5. implementazione, gestione e manutenzione dell'infrastruttura tecnologica.

3.2.2 Trattamento di dati personali finalizzato all'erogazione dei servizi sanitari socio-sanitari e socio-assistenziali all'interessato

3.2.2.1 Finalità e scenario complessivo

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 -per iniziativa personale o su indicazione di un soggetto sanitario- 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

ragioni culturali, linguistiche e socioeconomiche, che per il suo stato di salute- condizioni di coscienza e comprensione diverse: dalla completa incoscienza alla piena consapevolezza.

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, costituenti un **percorso** per scopi preventivi, curativi, riabilitativi, palliativi 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- qualificati come contitolari, titolari autonomi o responsabili

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 competenza e responsabilità- condividendo, mediante la trasmissione di documenti cartacei e/o informatici e/o mediante l'accesso controllato a sistemi informatici condivisi, i dati dell'interessato per costituire un unico

Nucleo di Riferimento complessivo del percorso diagnostico-terapeutico-assistenziale dell'interessato.

3.2.2.2 Principali attività che comportano l'accesso ai dati personali

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 cinque categorie:

1. La valutazione delle esigenze e l'effettuazione di atti sanitari, in presenza o in assenza[6] 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, contitolari o responsabili 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 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.

5. L'analisi e/o il trasferimento di dati personali -anche identificativi dell'interessato- a favore di Enti ed Istituzioni locali, regionali, statali, obbligatorio a fronte di specifiche disposizioni di legge, che definiscono nel dettaglio il tipo di dati da comunicare e le modalità di trasferimento.

[6] ad esempio nei casi di telemedicina, di tele-monitoraggio o di richiesta di supporto telefonico da parte dell'interessato stesso, per via telefonica o strumenti di comunicazione informatica

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

Le attività sono condotte sia mediante strumenti informatici che su supporto cartaceo, 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
- Valutazione generale dello stato del paziente (con particolare riguardo ai pazienti fragili e cronici) per l'individuazione di servizi preventivi nei vari centri (es. case della salute) collaboranti in un percorso territoriale

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 e, in generale, all'accesso del paziente nella struttura in vista dell'erogazione di servizi sanitari;
- Interazione con il paziente prima o dopo il contatto per definire aspetti organizzativi e logistici del servizio;
- Programmazione delle attività necessarie nei vari centri (es. case della salute) collaboranti in un percorso territoriale seguito da un paziente

Attività amministrative a fronte dei servizi erogati

- Invio di documenti al paziente e/o al medico di riferimento con modalità telematica o cartacea;
- 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 di prestazioni, effettuata anche in modalità telefonica e/o attraverso collaborazioni con strutture diverse sul territorio (es. farmacie)
- Fatturazione -individuale, 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 per fatti inerenti all'erogazione di servizi sanitari;
- Gestione pratiche legali ed istituzionali inerenti all'erogazione di servizi sanitari con conseguente de-archiviazione di dati personali
- Invio di documenti al paziente e/o al medico di riferimento con modalità telematica o cartacea;

Analisi e trasferimento dati a fronte di obblighi di legge

- Implementazione dei flussi informativi previsti dalle normative verso Enti ed Istituzioni locali, regionali, statali, per scopi di rendicontazione sulle attività effettuate e il supporto a decisioni di politica sanitaria da parte delle Istituzioni stesse.

3.2.2.3 Liceità del trattamento

La liceità del trattamento dei dati per l'erogazione dei servizi sanitari socio-sanitari e socio-assistenziali all'interessato si basa su e rispetta le seguenti discipline:

- art. 9 par. 1 lett. h) del Regolamento, sul trattamento per finalità di medicina preventiva o di medicina del lavoro, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali
- art. 2-sexies par. 2 lett. s) Codice Privacy relativo al trattamento dei dati nelle attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
- art. 2-sexies par. 2 lett. u) Codice Privacy; relativo al trattamento dei dati nello svolgimento dei compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
- misure di sicurezza ex art. 2-septies Codice privacy (in via di emanazione da parte del Garante Privacy);
- art. 75-_93 Codice privacy contenenti la disciplina specifica per il trattamento dei dati personali in ambito sanitario;
- inoltre i trattamenti dovranno tenere presenti i contenuti del Provvedimenti Garante Privacy che ai sensi dell'art. 22 comma 4 d.Lgs 101/2018 dovranno essere applicati ove ritenuti compatibili con il nuovo assetto del Regolamento

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

3.2.3.1 Finalità e scenario complessivo

A fronte di esigenze contingenti e/o nell'ambito di finalità istituzionali 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.

3.2.3.2 Liceità dei trattamenti

Per ogni trattamento implementato, il titolare definisce espressamente le finalità la liceità, dandone evidenza nel Registro dei trattamenti.

Ferma restando la necessità di valutazioni da effettuare in ogni singolo caso, i fondamenti di liceità di questa tipologia di trattamenti sono individuabili in:

- art. 9 par. 1 lett. h) del Regolamento, sul trattamento per finalità di medicina preventiva o di medicina del lavoro, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali
- art. 2-sexies par. 2 lett s) Codice Privacy relativo al trattamento dei dati nelle attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
- art. 2-sexies par. 2 lett u) Codice Privacy; relativo al trattamento dei dati nello svolgimento dei compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
- misure di sicurezza ex art. 2-septies Codice privacy (in via di emanazione da parte del Garante Privacy);
- inoltre i trattamenti dovranno tenere presenti i contenuti del Provvedimenti Garante Privacy che ai sensi dell'art. 22 comma 4 d.Lgs 101/2018 dovranno essere applicati ove ritenuti

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

3.2.4.1 Finalità e scenario complessivo

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 tre categorie:

a) trattamenti che non necessitano dell'identificazione della persona (e sono quindi basati su dati anonimi), finalizzati all'analisi dell'utenza, dei servizi erogati e delle attività espletate, a fini di decisioni organizzative interne;
b) trattamenti che non necessitano dell'identificazione della persona (e sono quindi basati su dati anonimi), finalizzati alla raccolta del livello di soddisfazione degli interessati in funzione del miglioramento continuo e/o alla comprensione del livello di percezione del clima organizzativo/aziendale;
c) trattamenti finalizzati alla interazione con i singoli interessati per scopi di fidelizzazione e presentazione/promozione di servizi;

3.2.4.2 Liceità dei trattamenti

Per ogni trattamento non basato su dati anonimi [7], il titolare definisce espressamente le finalità ed i criteri di liceità, dandone evidenza nel Registro dei trattamenti.

Ferma restando la necessità di valutazioni da effettuare in ogni singolo caso, i fondamenti di liceità di questa tipologia di trattamenti sono individuabili in:

- art. 9 par. 1 lett. h) del Regolamento, sul trattamento per finalità di medicina preventiva o di medicina del lavoro, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
- art. 2-sexies par. 2 lett. s) Codice Privacy relativo al trattamento dei dati nelle attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
- inoltre i trattamenti dovranno tenere presenti i contenuti del Provvedimenti Garante Privacy che ai sensi dell'art. 22 comma 4 d.Lgs 101/2018 dovranno essere applicati ove ritenuti compatibili con il nuovo assetto del Regolamento.

3.2.5 Trattamenti finalizzati alla ricerca scientifica

3.2.5.1 Finalità e scenario complessivo

Le attività di ricerca in campo medico e scientifico 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 (studi sperimentali);
Nota:
L'erogazione al paziente di tali atti sanitari particolari è subordinata ad una esplicita accettazione del paziente.

b) effettuazione di analisi massive su tutti i dati disponibili di più pazienti (anonimizzati o meno) al fine di verificare e/o individuare correlazioni fra i dati stessi e di derivare informazioni utili dal punto di vista scientifico (studi osservazionali).

7 Non rientrante quindi negli ambiti di applicabilità del regolamento e citato in questa sede solo per completezza di documentazione

3.2.5.2 Liceità dei trattamenti

Per ogni trattamento non basato su dati anonimi[8], il totale definisce espressamente le finalità ed i criteri di liceità, dandone evidenza nel Registro dei trattamenti.

Ferma restando la necessità di valutazioni da effettuare in ogni singolo caso, i fondamenti di liceità di questa tipologia di trattamenti sono individuabili in:

- art. 9 par. 1 lett. j) del Regolamento, sul trattamento per finalità di ricerca scientifica;
- art. 89 del Regolamento che elenca le garanzie e deroghe relative al trattamento a fini di ricerca scientifica;
- art. 110 del Codice Privacy relativo alla Ricerca medica, biomedica ed epidemiologica;
- art. 110 -bis del Codice Privacy relativo al Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici;
- Regole deontologiche per trattamenti ai fini statistici o di ricerca scientifica (pubblicate nella G.U. del 14 gennaio 2019 n. 11);
- Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (allo stato attuale in consultazione pubblica).

3.2.6 Trattamenti finalizzati alla gestione della infrastruttura tecnologica

3.2.6.1 Finalità e scenario complessivo

L'infrastruttura tecnologica implementata dal titolare -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. La complessità di questa infrastruttura e la sua rilevanza ai fini dei processi clinici, assistenziali ed organizzativi è in continua crescita.

Le relative attività di implementazione, gestione, manutenzione sono eseguite -localmente o in cloud- da personale dell'organizzazione del titolare nominato quale autorizzato (ex art 29 del Regolamento) ed al quale sono state date apposite istruzioni, oppure da singoli professionisti e/o personale afferente all'organizzazione di soggetti esterni nominati dal titolare quali responsabili (ex art. 28 del Regolamento) e con i quali è stato stipulato apposito contratto nel quale è definito l'oggetto del

8 Non rientrante quindi negli ambiti di applicabilità del regolamento e citato in questa sede solo per completezza di documentazione

trattamento, e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Gli ambienti tecnologici usualmente prevedono una figura di "amministratore" che ha accesso a tutte le risorse e tutti i dati del sistema.

4. Implementazione di un "Sistema di gestione per la protezione dei dati personali"

4.1 Struttura organizzativa

Il titolare stabilisce, documenta, attua e mantiene attivo un "Sistema di gestione per la protezione dei dati personali" ed opera per migliorarne in continuo l'efficacia, in accordo con i principi e gli obblighi previsti dal Regolamento e delle normative di rilevanza.

Tenendo conto dei molteplici aspetti e requisiti (clinici, etici, sociali, organizzativi, economici) delle organizzazioni sanitarie, per la definizione, gestione, valutazione ed evoluzione del Sistema per la protezione dei dati personali il titolare istituisce un "Comitato per la protezione dei dati personali" che si avvale -oltre che del Responsabile della Protezione Dati, il cui ruolo e responsabilità sono definiti dal Regolamento- del contributo di referenti dell'organizzazione almeno relativamente alle seguenti aree (ferma restando la possibilità di ulteriori apporti derivanti dallo specifico contesto di attività del titolare, incluso il caso di attività effettuate mediante l'ausilio di responsabili del trattamento):

a) l'area sanitaria, con particolare riferimento ai requisiti dei processi sanitari, alle esigenze mediche ed assistenziali ed al rischio clinico;
b) l'area amministrativa;
c) l'area di implementazione e di gestione del sistema informativo, dell'infrastruttura tecnologica e dei dispositivi medici.

Responsabilità del Comitato per la protezione dei dati personali

Il Comitato per la protezione dei dati personali è responsabile di:

a) promuovere, redigere e/o validare la documentazione del Sistema per la protezione dei dati (cfr. § 4.2);
b) fornire consulenza alle varie aree dell'organizzazione in merito alla protezione dei dati personali, assicurando una visione complessiva che tenga conto di tutte le esigenze dell'organizzazione;
c) validare le procedure organizzative e le soluzioni tecnologiche implementate presso l'organizzazione relativamente agli aspetti di protezione dei dati personali e dei rischi connessi;

d) analizzare i risultati degli audit interni (cfr. § 4.3) e definire/validare le eventuali azioni correttive necessarie;
e) valutare periodicamente le caratteristiche del Sistema di gestione per la protezione dei dati e proporre alla Direzione i piani evolutivi necessari assicurarne la continua efficacia ed idoneità rispetto alle esigenze dell'organizzazione.

Responsabilità della Direzione
La Direzione assicura il proprio impegno per lo sviluppo e per l'attuazione del Sistema per la protezione dei dati personali e per migliorare in continuo la sua efficacia:
a) verificando inizialmente, anche attraverso il Comitato per la protezione dei dati personali, che il sistema nel suo complesso sia idoneo, adeguato ed efficace rispetto al dettato normativo ed agli interessi e le finalità dell'organizzazione;
b) comunicando a tutto il personale l'importanza di soddisfare i requisiti di protezione dei dati personali ed assicurando necessaria formazione a tutti gli operatori;
c) assicurando che siano effettuati riesami e valutazioni periodiche delle singole componenti individuali del Sistema per la protezione dei dati personali, verificandone l'idoneità e individuando obiettivi e piani di miglioramento;
d) effettuando riesami periodici del Sistema nel suo complesso per verificarne la continua coerenza e la continua idoneità, adeguatezza ed efficacia rispetto al dettato normativo ed agli interessi e le finalità dell'organizzazione, e valutando opportunità di miglioramento ed esigenza di modifiche.

Di tutti i riesami effettati viene mantenuta evidenza.

Nota
Il presente modello si intende finalizzato alla valutazione complessiva di tutte le esigenze e tutti gli aspetti dell'organizzazione sanitaria e va inteso quindi applicabile anche in organizzazioni di dimensioni ridotte in cui non sia presente una netta separazione delle strutture operative e dei ruoli individuali.

4.2 Documentazione di riferimento

L'approccio e le soluzioni -organizzative, tecnologiche e manuali- adottati dall'organizzazione per la protezione dei dati sono definiti in un insieme omogeneo e coerente di documenti -preferibilmente in forma informatizzata-, in modo da disporre di un quadro complessivo di riferimento, minimizzando il rischio di incoerenze e di errori di comunicazione e di interpretazione all'interno della struttura e sulla base del quale effettuare le valutazioni dei rischi ed i programmi evolutivi.

Va inoltre osservato come, anche all'interno della stessa organizzazione, l'infrastruttura tecnologica sia articolata in diversi sistemi informatizzati, utilizzati per specifiche attività e variamente interconnessi per il supporto ai vari processi. Conseguentemente anche i dati sono in gran parte distribuiti (financo replicati) fra sistemi diversi, forniti da produttori diversi e organizzati secondo strutture diverse e proprietarie.

Al fine di poter assicurare una adeguata protezione, è pertanto essenziale che il Sistema di protezione dei dati personali contenga, oltre alle regole di comportamento definite dall'organizzazione, anche procedure e documenti che consentano di:

a) disporre di un quadro completo delle caratteristiche e delle possibilità offerte dai vari sistemi informatizzati in termini di protezione dei dati personali, con gli eventuali rischi;
b) poter definire, monitorare e misurare l'evoluzione di piani miglioramento coerenti, organici e basati sui rischi dei vari settori e sulle priorità dell'organizzazione.

Con questi fini, il titolare redige -attraverso il Comitato per la protezione dei dati personali- un "**Manuale di riferimento per la protezione dei dati personali**" nel quale sono complessivamente descritti:

a) le aree di applicazione del sistema di protezione dei dati personali, compresi dettagli e giustificazioni relativamente ad eventuali esclusioni;
b) le regole di operatività del "Comitato per la protezione dei dati";
c) i principi e le soluzioni (organizzative, tecnologiche e manuali) adottate per il controllo ed il miglioramento continuo del sistema di protezione dei dati;
d) i riferimenti alle procedure organizzative e di formazione definite dal titolare in merito alla protezione dei dati nell'ambito dei trattamenti implementati.

Oltre al "Manuale di riferimento per la protezione dei dati", fanno parte della documentazione del Sistema di gestione per la protezione dei dati personali:

a) tutti i documenti espressamente richiesti dal Regolamento;

b) gli atti formali mediante i quali sono designati il Responsabile della protezione dei dati ed i partecipanti del Comitato per la protezione dei dati;

c) il **"Livello di adozione del codice di condotta":** documento che specifica le prescrizioni di questo codice di condotta che sono al momento adottate dal titolare;

d) il "**Registro dei sistemi informatizzati**": documento che contiene l'elenco dei sistemi informatizzati (inclusi i dispositivi medici) utilizzati nell'ambito dei trattamenti, corredato di alcuni indicatori circa le caratteristiche dei

sistemi stessi in merito alla protezione dei dati secondo le indicazioni definite in questo codice;

e) il **"Registro dei profili di abilitazione"**: documento che contiene l'elenco dei profili di abilitazione definiti nei singoli sistemi informatizzati con la individuazione dei relativi privilegi, secondo le indicazioni fornite in questo codice;

f) i documenti, le procedure e le registrazioni definite in questo Codice di condotta;

g) le procedure organizzative e di formazione rilevanti in termini di protezione dati, definite dal titolare in merito alla esecuzione dei vari trattamenti, sia relativamente alle attività informatizzate che a quelle manuali;

h) le registrazioni predisposte per verificare e per fornire evidenza della conformità ai requisiti e dell'efficace funzionamento del sistema di gestione per la protezione dei dati;

i) tutti gli altri documenti che il titolare ritiene necessari per assicurare l'efficace pianificazione, funzionamento e tenuta sotto controllo del sistema.

I documenti e le registrazioni sono tenuti sotto controllo. Il titolare definisce una procedura per stabilire le modalità di controllo necessarie per l'identificazione, l'archiviazione, la protezione, il reperimento, la conservazione e l'eliminazione delle registrazioni. I documenti e le registrazioni devono rimanere leggibili, facilmente identificabili e reperibili.

La documentazione del Sistema di gestione per la protezione dei dati personali è resa disponibile alla Autorità di controllo ed agli eventuali enti certificatori.

4.3 Verifiche periodiche

Il titolare conduce ad intervalli pianificati audit interni per determinare se il sistema per la protezione dei dati:

a) è conforme a quanto pianificato, ai requisiti normativi ed ai requisiti del sistema di gestione per la protezione dei dati stabiliti dall'organizzazione stessa;
b) è efficacemente attuato e mantenuto.

A tal fine, il Comitato per la protezione dei dati:

a) definisce una procedura per stabilire le responsabilità ed i requisiti per la pianificazione e per la conduzione degli audit per i vari componenti del sistema e per predisporre le relative registrazioni;

b) definisce periodicamente un programma di audit che prenda in considerazione lo stato e l'importanza dei processi e delle aree da sottoporre ad audit, così come i risultati di audit precedenti, definendo i criteri, il campo di applicazione, la frequenza ed i metodi degli audit.

La scelta degli auditor e la conduzione degli audit devono assicurare l'obiettività e l'imparzialità del processo di audit. Gli auditor non devono effettuare audit sul proprio lavoro.

Sono mantenute registrazioni degli audit e dei loro risultati; le registrazioni degli audit sono trasmesse al Comitato per la protezione dei dati.

La direzione responsabile dell'area sottoposta ad audit deve assicurare che ogni correzione ed azione correttiva necessarie per eliminare le non conformità rilevate e le loro cause vengano effettuate senza indebito ritardo. Le attività successive devono comprendere la verifica delle azioni effettuate ed il rapporto sui risultati della verifica

4.4 Formazione

Il titolare definisce procedure al fine di assicurare una adeguata formazione sui principi del Regolamento e sulle regole adottate nell'organizzazione stessa, sia al personale interno che ad operatori esterni che collaborino nell'ambito delle attività.

La formazione comprende sia una fase iniziale, al momento dell'inizio della collaborazione, sia momenti periodi di verifica ed aggiornamento definiti secondo un piano annuale.

Le verifiche periodiche di cui al precedente §4.3 comprendono anche la valutazione dell'efficacia della formazione effettuata.

4.5 Monitoraggio

Il titolare applica metodi adeguati per monitorare e, ove possibile, misurare i diversi aspetti (processi organizzativi e gli strumenti tecnologici) interessati dal sistema per la protezione dei dati. Questi metodi devono verificare e dimostrare la capacità dei processi e degli strumenti di assicurare il rispetto delle regole e delle procedure definite. Qualora tale rispondenza non risulti dimostrata, devono essere intraprese correzioni ed azioni correttive, per quanto appropriato.

Nel determinare i metodi adeguati al monitoraggio dei singoli aspetti di interesse, è consigliabile che il titolare prenda in considerazione le caratteristiche degli aspetti stessi in relazione al loro impatto in termini di rischi e di efficacia del sistema nel suo complesso.

4.6 Rapporti con i responsabili del trattamento

Il rapporto stipulato fra il titolare ed un responsabile del trattamento ai sensi dell'Articolo 28.3 del Regolamento include l'impegno da parte del responsabile ad applicare le regole di questo codice di condotta, l'adozione da parte del responsabile delle procedure del sistema di gestione per la protezione dei dati personali implementato dal titolare e la collaborazione nella esecuzione e/o l'esecuzione autonoma delle attività previste, dandone evidenza al titolare.

Per semplicità espressiva, nel seguito di questo documento si farà sempre riferimento al titolare, fermo restando che singole attività -dettagliatamente specificate nel contratto di collaborazione- possono essere in tutto o in parte delegate al responsabile.

Il Titolare mantiene comunque sempre la responsabilità di monitorare, di verificare periodicamente e di approvare -dandone evidenza- le attività effettuate dal Responsabile.

4.7 Aree di responsabilità previste dal Regolamento non esplicitamente dettagliate in questo codice

Nell'ambito del Sistema di gestione per la protezione dei dati personali, il titolare definisce procedure anche per gli altri obblighi previsti dal Regolamento per i quali il presente codice non fornisce indicazioni specifiche.

5. Rapporti con l'interessato

5.1 Informativa all'interessato

Il titolare definisce una procedura relativamente ai contenuti dell'informativa ed alle modalità di comunicazione all'interessato.

5.1.1 Contenuto

L'informativa contiene le informazioni di cui agli articoli 13 e 14 del regolamento e viene redatta secondo le indicazione delle Linee Guida elaborate dal Gruppo Art. 29 [9] in materia di trasparenza (documento WP 260 [10]), definite in base alle previsioni del Regolamento.

Nell'informativa sono descritte le tipologie di trattamento effettuate dal titolare, come indicate al § 3.2.1.

9 Rinominato dal 25.5.2018 "Comitato europeo per la protezione dei dati", https://edpb.europa.eu/edpb_it

10 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Nell'informativa è evidenziato che i trattamenti finalizzati a scopo statistico ed epidemiologico a fini di prevenzione comportano la profilazione dell'interessato (art. 15 del Regolamento), ma che vengono basati sulla pseudonimizzazione e che -solo nel caso si riscontrino rischi per l'interessato stesso- questo viene identificato ed avvertito, seguendo una procedura stabilita dal titolare.

Nell'informativa è anche evidenziato che i trattamenti effettuati del titolare a fini di ottimizzazione della propria struttura ed offerta di servizi possono comportare la profilazione (art. 15 del Regolamento), ma che -in tal caso- si basano sulla pseudonimizzazione e che eventuali attività di identificazione dell'interessato sono finalizzate soltanto alla comunicazione con lo stesso per la promozione di nuovi servizi da parte del titolare.

5.1.2 Modalità di comunicazione

L'informativa all'interessato è resa nota almeno in tutte le seguenti forme:

a) è pubblicata, in posizione evidente e facilmente raggiungibile sul sito web dell'organizzazione;
b) è affissa in modo evidente, ed è fornita su supporto cartaceo a fronte di richiesta dell'interessato, negli uffici dell'organizzazione dedicati alle relazioni amministrative con i pazienti (es. accettazione, prenotazione ambulatoriale, URP, etc.)

Per quanto possibile, il riferimento alla pagina del sito contenente l'informativa è stampato sui documenti amministrativi forniti all'interessato all'inizio di un contatto (es. prenotazione, presa in carico, accettazione, etc.).

5.2 Acquisizione del consenso

Il consenso dell'interessato acquisto, relativamente ai trattamenti per i quali è necessario e si intende a tempo indeterminato, fino ad esplicita revoca da parte dell'interessato.

5.2.1 Trattamenti per i quali è necessario il consenso

Il consenso dell'interessato è necessario e quindi viene acquisito:

a) relativamente ai trattamenti finalizzati ad analisi a supporto di decisioni del titolare in merito alla propria attività (cfr. § 3.4), basati su dati non psudonomizzati e che possano determinare contatti del titolare con l'interessato per la fidelizzazione, per la promozione e per comunicazioni in merito a servizi offerti dal titolare.

b) relativamente alla condivisione dei dati con strutture e professionisti non appartenenti all'organizzazione del titolare ma cooperanti nella cura e nell'assistenza al paziente nell'ambito di dell'erogazione dei servizi sanitari necessari al paziente anche nell'ambito un percorso territoriale finalizzato alla prevenzione, cura o assistenza [11].

Non richiede l'acquisizione del consenso, ma solo la menzione nell'informativa, la comunicazione e condivisione dei dati fra il Nucleo di riferimento ed il Medico di Medicina Generale responsabile del paziente [12] e la comunicazione di dati ad altre strutture alle quali vengano richieste prestazioni o nelle quali venga trasferito il paziente nell'ambito o a seguito di un contatto.

5.2.2 Modalità di acquisizione del consenso

Il consenso viene acquisito:

a) mediante la sottoscrizione da parte del paziente di un modulo cartaceo controfirmato dal rappresentante del titolare che ha acquisito il consenso stesso, scansionabile e conservabile in sola forma informatica;
b) mediante un documento informatico firmato con firma digitale da parte del paziente;
c) mediante un video nel quale il paziente esprima chiaramente il consenso;
d) tramite un sito al quale l'assistito possa accedere mediante credenziali ottenute a seguito di un processo di identificazione personale, mediante la conferma da parte dell'assistito stesso di appositi campi in una pagina web o mediante il caricamento di un documento firmato e scansionato o mediante l'utilizzo di una app;
e) mediante un documento firmato e scansionato dal paziente, inviato dal paziente stesso mediante posta elettronica certificata, dei cui riferimenti il titolare tiene traccia.

5.2.3 Consenso nel caso dei minori

In caso di minori, il consenso deve essere acquisito da chi esercita la potestà legale sull'interessato. In caso di minori, una volta raggiunta la maggiore età, il consenso dell'interessato deve essere acquisito nuovamente.

5.2.4 Evidenza dell'avvenuta acquisizione del consenso

11 *Art. 34 Codice deontologia medica: "L'informazione a terzi può essere fornita previo consenso esplicitamente espresso dalla persona assistita, fatto salvo quanto previsto agli artt. 10 e 12, allorché sia in grave pericolo la salute o la vita del soggetto stesso o di altri".* https://portale.fnomceo.it/codice-deontologico/

12 *Art. 42 comma 2 lettera a del nuovo Accordo collettivo nazionale per la disciplina dei rapporti con i medici di medicina generale 23.03. 2005 che stabilisce che il MMG dovrebbe essere comunque in stretto collegamento con i medici del reparto e garantire la trasmissione di più informazioni possibili sul paziente*

Il titolare tiene registrazione dell'avvenuta acquisizione del consenso in un archivio centralizzato, preferibilmente in forma informatizzata.

5.3 Diritto dell'interessato all'accesso ai dati ed alla portabilità degli stessi

5.3.1 Informazioni fornite all'interessato

Il titolare definisce una procedura secondo cui fornire all'interessato, a fronte di una richiesta dello stesso, le informazioni di cui agli Articoli 13 e 14 ed ai paragrafi 1 e 2 dell'Articolo 15 del Regolamento.

5.3.2 Accesso ai dati e portabilità degli stessi

I sistemi informatizzati in uso all'interno delle singole organizzazioni sanitarie sono fortemente differenziati sia in termini di disponibilità di funzioni per l'esportazione dei dati di un paziente, sia in termini di formati, completezza, sintassi e semantica di tali eventuali esportazioni.

Ciò rende molto difficile, spesso impossibile, consentire all'interessato sia l'accesso a tutti dati gestiti secondo quanto previsto al punto 3 dell'articolo 15 del Regolamento, che l'estrazione e l'organizzazione degli stessi secondo un formato strutturato ed omogeneo utilizzabile mediante strumenti automatici utilizzabili dall'interessato e/o da parte di terzi ai quali l'interessato voglia comunicarli, secondo quanto previsto all'Articolo 20 del Regolamento.

Per far fronte a questo obiettivo, il titolare si impegna:

a) a far sì che tutti i nuovi sistemi dispongano di una funzionalità per l'esportazione dei dati -sia documenti che informazioni elementari- dei pazienti gestiti dal sistema stesso secondo formati strutturati, il più possibile basati su standard riconosciuti;

b) a definire le caratteristiche di un modello di riferimento unificato secondo il quale integrare ed armonizzare i dati provenienti dai diversi sistemi e rendere quindi disponibile al paziente l'insieme dei dati gestiti, secondo i requisiti espressi all'Articolo 20 del Regolamento.

La strategia individuata per il raggiungimento di tale obiettivo ed il piano per l'implementazione sono registrate in un apposito documento del Sistema per la protezione dei dati personali.

5.4 Diritto dell'interessato alla cancellazione

Purché non in concomitanza con l'erogazione di servizi sanitari da parte del titolare all'interessato, l'interessato ha diritto di richiedere la cancellazione totale o parziale dei propri dati in possesso del titolare.

Considerato che:

a) per alcuni dati raccolti dal titolare (cartelle cliniche e, secondo l'accezione attualmente prevalente, tutte le registrazioni cliniche) esistono obblighi di legge che ne prescrivono la conservazione;
b) la conservazione dei dati è necessaria al titolare per la tutela dei propri diritti legali e di difesa, in caso di contestazioni da parte dell'interessato e delle Autorità;

la cancellazione richiesta dall'interessato viene implementata nella non disponibilità e nella non accessibilità dei dati dell'interessato nei processi sanitari, amministrativi ed organizzativi del titolare, ma non nella distruzione fisica dei dati stessi.

I dati rimangono disponibili nella loro interezza per le sole finalità di cui ai precedenti punti a) e b). Il titolare ha facoltà di mascherarli in modo da non rendere in alcun modo possibile l'identificazione dell'interessato ed utilizzarli per soli trattamenti finalizzati a scopi statistici, epidemiologici e di ricerca.

5.5 Diritto dell'interessato alla rettifica

La rettifica di dati che sono stati frutto di valutazioni cliniche e/o esami diagnostici effettuati da parte del titolare o da parte di altre strutture sanitarie può essere richiesta dall'interessato solo a fronte della presentazione di documentazione clinica rilasciata da un altro professionista abilitato, a fronte della quale il titolare effettua le opportune verifiche ed indagini per individuare le cause di discordanza, informando l'interessato delle risultanze ottenute.

La rettifica di dati -anche inerenti allo stato di salute- forniti autonomamente dall'interessato sotto la propria responsabilità e senza il supporto di una documentazione clinica redatta da un professionista abilitato può essere richiesta direttamente dall'interessato, senza bisogno di documentazione aggiuntiva.

Nel caso in cui vengano rettificati dati inerenti alla salute dell'interessato, la responsabilità del titolare sui servizi sanitari erogati e per i quali i valori rettificati possono essere rilevanti si intende solo successivamente alla rettifica stessa.

Il titolare conserva in ogni caso copia del valore precedente alla rettifica registrando la data della rettifica stessa, in quanto tale valore precedente è potenzialmente rilevante rispetto alle decisioni mediche prese fino al momento della rettifica ed alle conseguenti responsabilità.

5.6 Obbligo di notifica in caso di cancellazione o rettifica

Relativamente ai dati gestiti mediante i sistemi informatizzati dotati delle caratteristiche di tracciamento degli accessi descritte al § 7.3, il titolare notifica -anche mediante strumenti automatici dotati delle adeguate garanzie di sicurezza-

eventuali cancellazioni o rettifiche dei dati a tutti gli utenti esterni all'organizzazione che abbiano fatto accesso e/o a cui siano stati trasmessi i dati rettificati e/o cancellati. Su richiesta dell'interessato, comunica allo stesso la lista dei destinatari della notifica.

Relativamente ai dati gestiti mediante documenti cartacei e/o mediante sistemi informatizzati non dotati delle caratteristiche di tracciamento descritte al § 7.3, il titolare valuta lo sforzo necessario per la notifica della cancellazione/rettifica, decidendo di conseguenza.

Su richiesta dell'interessato, comunica allo stesso l'esito della valutazione e le eventuali azioni intraprese.

La notifica o l'esito della valutazione viene registrato.

6. Necessità e criteri per l'accesso e l'utilizzo dei dati

6.1 Necessità e accessibilità ai dati nell'ambito dei trattamenti

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

6.1.1.1 Tipologie di dati necessari

a. 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.

Il personale medico ed assistenziale interessato all'effettuazione di atti sanitari nei confronti del paziente comprende personale dell'organizzazione del titolare, consulenti esterni operanti presso la struttura del titolare, personale di altre strutture e singoli professionisti operanti sul territorio che abbiano regolarmente in cura il paziente (es. il medico di medicina generale e specialisti di determinate patologie di cui soffre il paziente) e/o che collaborino formalmente nell'ambito del percorso di cura seguito dal paziente stesso. Il rapporto di collaborazione con strutture esterne e singoli professionisti -in qualità di contitolari o titolari autonomi- viene formalizzato.

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.

Eventuali dati clinici dell'interessato che evidenzino stati di salute e situazioni che possano determinare rischi per la salute degli operatori coinvolti nell'effettuazione di prestazioni ed atti sanitari devono essere evidenziati e comunicati agli operatori stessi, compatibilmente con le disposizioni di legge applicabili.

b. 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.

c. 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.

d. 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.

e. Attività obbligatorie a fronte di specifiche previsioni normative concernenti analisi statistiche finalizzate a decisioni di politica sanitaria
I dati necessari da fornire e/o elaborare nelle attività obbligatoriamente implementate dal titolare in ottemperanza a quanto previsto dalle disposizioni di legge sono definiti nelle disposizioni stesse.
Anche in funzione dei sistemi informatizzati in uso, le informazioni necessarie non sono sempre disponibili in forma disaggregata, ma può risultare l'analisi e la correlazione di altri dati personali per ottenere quanto prescritto.
In via generale, quindi, per ottemperare a queste disposizioni si può prevedere la necessità di accedere a tutte le informazioni (anche identificative) sul paziente.

6.1.1.2 Criteri di abilitazione all'accesso

a. Il personale del "Nucleo di riferimento" responsabile del coordinamento dei servizi sanitari ha accesso -secondo i criteri esposti nel § 6.1.1.a- ai dati personali dei soli pazienti di cui ha la responsabilità e per la sola durata del contatto.

   Nell'ambito del percorso di cura di un paziente hanno accesso ai dati personali dello specifico paziente i singoli professionisti ed i "Nuclei di riferimento" delle organizzazioni che cooperano nella cura e nell'assistenza al paziente durante il percorso stesso.

   La collaborazione con strutture e professionisti esterni all'organizzazione del titolare nella gestione di un percorso del paziente viene definita dall'organizzazione mediante atto formale che stabilisca i ruoli (contitolare, titolare autonomo, responsabile) e viene verificata con frequenza periodica secondo una procedura. L'esito della verifica viene registrato e può dare adito a modifiche nei criteri di abilitazione all'accesso ai sistemi informatizzati.

   La composizione del Nucleo di riferimento (o dei Nuclei di riferimento in caso di collaborazione fra più organizzazioni) viene registrata e mantenuta aggiornata, sia relativamente alle Unità Organizzative delle organizzazioni coinvolte, sia relativamente ai singoli professionisti operanti individualmente.

b. I destinatari delle richieste di prestazioni per un interessato (singoli individui o personale della Unità Organizzativa), hanno accesso -secondo i criteri esposti nel § 6.1.1.a- ai dati personali dei soli pazienti per i quali viene fornita 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 § 6.1.1.c- 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 § 6.1.1.d- ai dati personali dei pazienti per i quali, al momento sia in corso o sia previsto un contatto.

e. Il personale preposto ai trattamenti comprendenti dati personali anche identificativi dell'interessato ed obbligatoriamente implementati dal titolare in attuazione di disposizioni di legge è individualmente e specificatamente autorizzato.

6.1.1.3 Esigenze particolari

a. Il personale medico facente parte del "Nucleo 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 ed è 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 § 6.1.1.1.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'autorità giudiziaria, dell'interessato e/o di un altro operatore sanitario che ha al momento in cura il paziente e/o da parte del paziente stesso.

In qualsiasi momento -senza limiti temporali- professionisti della struttura del titolare possono ricevere la richiesta di dati personali raccolti durante l'erogazione di servizi sanitari erogati in precedenza all'interessato:

1. da parte dell'autorità giudiziaria per motivi legali;
2. da parte di strutture o singoli professionisti al momento impegnati nell'erogazione di servizi sanitari all'interessato al fine di valutare lo stato di salute dell'interessato ed assicurare la sicurezza e l'appropriatezza del servizio sanitario da questi erogato.

Possono anche ricevere da parte dell'interessato stesso richieste finalizzate ad ottenere pareri e/o indicazioni sul suo stato di salute e/o su terapie/trattamenti in corso.

In tali situazioni, e per il solo periodo di tempo necessario per l'esaudimento della richiesta, questi professionisti hanno necessità di accedere, secondo i criteri esposti nel § 6.1.1.1.a, a tutte le informazioni della persona oggetto della richiesta.

L'accesso effettuato in tali circostanze viene registrato con le relative motivazioni.

c. Esportazioni massive di dati personali dai sistemi informatizzati

Nell'ambito delle alcune attività (in particolare di quelle relative alla pianificazione) può risultare utile avvalersi di strumenti e procedure informatiche diverse (esempio fogli Excel) esportando i dati dai sistemi informatizzati di supporto al processo.

L'attivazione di eventuali funzionalità esportazione massiva dai sistemi informatizzati è riservata a personale appositamente autorizzato e viene definita una procedura circa la tenuta, la conservazione, la diffusione e la distruzione di tali dati esportati.

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

6.1.2.1 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 l'identificazione degli interessati, ma è sufficiente poter collegare i dati a generici soggetti anonimi, purché sia garantita l'unicità del soggetto 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 e da poter eseguire quanto necessario, nell'interesse degli stessi e della collettività.

Questi trattamenti vengono pertanto eseguiti su dati psudonimizzati secondo i criteri indicati al § 7.5.

6.1.2.2 Criteri di abilitazione all'accesso

I ricercatori -personale tecnico e sanitario- responsabili delle analisi hanno accesso a tutte le informazioni disponibili pseudonimizzate, (che non consentono -si ripete- l'individuazione diretta 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, mediante le procedure e misure di sicurezza indicate al successivo § 7.5 ed annotata in appositi registri.

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

6.1.3.1 Tipologie di dati necessari

a) trattamenti 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.
   Questi trattamenti si basano pertanto su dati resi anonimi.

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 di 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, da specificarsi nella descrizione del trattamento redatta nel "Registro dei trattamenti"

6.1.3.2 Criteri di abilitazione all'accesso

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

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

6.1.4 Trattamenti finalizzati alla ricerca scientifica.

6.1.4.1 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 § 3.2.1, 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 § 7.1.1.

   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 e che includano -fra le altre- anche la finalità di poter individuare situazioni di rischio o di rilevanza nell'interesse della singola persona.

   Questi trattamenti sono eseguiti con strumenti informatici, e -di norma- 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 l'identificazione degli interessati, ma è sufficiente poter collegare i dati a generici soggetti anonimi, purché sia garantita l'unicità del soggetto 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.

Questi trattamenti vengono pertanto eseguiti su dati psudonimizzati secondo i criteri indicati al § 7.5.

c) 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 e che non includano -fra le altre- anche la finalità di poter individuare situazioni di rischio o di rilevanza nell'interesse della singola persona.

Questi trattamenti vengono eseguiti su dati resi completamente anonimi.

6.1.4.2 Criteri di abilitazione all'accesso

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 § 3.2.1. Si applicano quindi i criteri di abilitazione descritti al § 7.1.2.2

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).

In quei trattamenti, basati su dati pseudonimizzati che prevedono -fra le finalità- la identificazione della persona, '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, mediante le procedure e misure di sicurezza indicate al successivo § 7.5 ed annotata in appositi registri.

c) 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, e che non includano -fra le altre- anche la finalità di poter individuare situazioni di rischio o di rilevanza nell'interesse della singola persona.

Tali trattamenti sono basati esclusivamente su dati anonimi e pertanto 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.

6.1.5 Trattamenti finalizzati alla gestione della infrastruttura tecnologica

6.1.5.1 Tipologie di dati necessari

Nell'ambito dei processi implementati dal titolare per la attivazione, 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 permessi 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.

6.1.5.2 Criteri di abilitazione all'accesso

Il personale preposto ai trattamenti che comportino -direttamente (caso 6.1.6.1a) o indirettamente (caso 6.1.6.1.b)- l'accesso ai dati personali dell'interessato ha accesso a tutte le informazioni personali registrate nel sistema secondo opportune regole di abilitazione e -qualora la tecnologia lo supporti- con l'attivazione di meccanismi di registrazione delle attività effettuate.

Qualora la tecnologia dei sistemi interessati supporti meccanismi di mascheramento dinamico dei dati identificativi, i profili di abilitazione del personale incaricato di queste attività saranno configurati per consentire l'accesso ai dati tramite questi filtri.

6.2 Regole di protezione predefinita

E' impegno del titolare implementare i criteri indicati al paragrafo precedente quali regole di protezione predefinita nei sistemi informatici di nuova realizzazione.

Relativamente ai trattamenti già in essere finalizzati a scopi statistici, di prevenzione e di ricerca (come descritti ai § 6.1.2, 6.1.3, 6.1.4.b e 6.1.4.c), l'organizzazione definisce ed implementa un piano di evoluzione che porti gli stessi ad operare secondo gli scenari descritti.

La caratteristica del sistema informatizzato di operare su dati identificativi, psudonomizzati o anonimi viene evidenziata nel Registro dei sistemi informatizzati.

A complemento e dettaglio dei criteri di abilitazione predefinita, è impegno dell'organizzazione dotare i sistemi informatizzati della possibilità di definire profili di abilitazione mediante i quali dettagliare i privilegi dei diversi ruoli professionali in termini di funzionalità eseguibili e di dati accessibili nell'ambito dello specifico sistema. Ogni persona può avere diversi profili di abilitazione, in funzione dei diversi ruoli nei singoli contesti dell'organizzazione e delle diverse situazioni e contingenze che possono verificarsi (es. emergenze, guardie, etc.).

Nei sistemi informatizzati già esistenti, dotati della sola generica possibilità di definire meccanismi di abilitazione differenziata in funzione di diversi profili di utenza, questi criteri sono tradotti -per quanto possibile- nelle regole di abilitazione dei profili dei singoli sistemi.

Il caso di sistemi informatizzati già esistenti, non dotati della possibilità di definire profili di abilitazione differenziati in funzione dell'utenza, viene

evidenziato nel "Registro dei sistemi informatizzati", insieme ad una valutazione del rischio e -se necessario e possibile- ad un piano evolutivo per aggiornare il sistema.

Nel "Registro dei sistemi informatizzati", vengono evidenziate le possibilità offerte dai singoli sistemi in termini di abilitazione all'accesso ai dati, ovvero:

a) accessibilità pre-definita secondo i criteri esposti nel § 6.1 (con l'eventuale specifica di ulteriori dettagli mediante la definizione di profili di abilitazione aggiuntivi per i diversi ruoli);
b) accessibilità mediante profili di abilitazione, specificando la possibilità di configurare i profili stessi in modo da rispondere ai criteri di abilitazione di riferimento definiti nel § 6.1 (*preferibilmente secondo una scala "Alto" / "Medio" / "Basso" ed esplicitando gli eventuali fattori di incompatibilità*);
c) impossibilità di definire criteri di accessibilità diversificati per i diversi utenti;
d) capacità di esportare/importare i profili di abilitazione e le utenze collegate, in modo da consentire una gestione complessiva e centralizzata di queste informazioni.

Per l'esecuzione di attività che facciano uso di documenti cartacei contenenti dati personali, il titolare definisce delle procedure organizzative per l'accesso e la consultazione degli stessi conformemente ai criteri definiti. Sono parimenti definite ed implementate delle regole per il trasporto dei documenti cartacei in modo da ridurre il rischio di accesso ai dati da parte di persone non autorizzate.

6.3 Abilitazione individuale all'accesso ai dati

6.3.1 Criteri generali

Per ogni sistema informatizzato, il titolare definisce dei "profili di abilitazione" relativi ai ruoli professionali coinvolti, associando ad ognuno di questi le attività eseguibili ed i dati accessibili.

I profili possono essere applicabili:

a) nell'ambito di unità organizzative della struttura, nel qual caso consentono l'accesso e l'operatività -secondo le regole definite- relativamente a tutti i pazienti in carico a quella unità organizzativa;

b) relativamente a singoli pazienti, nel qual caso consentono l'accesso e l'operatività -secondo le regole definite- relativamente ai soli pazienti esplicitamente individuati (il caso tipico è quello di organizzazioni e professionisti esterni che collaborano nella attuazione di un percorso di cura e assistenziale del paziente).

Le persone fisiche operanti con i singoli sistemi informatizzati sono individualmente associate ai profili di abilitazione di pertinenza, per un periodo temporale non indefinito. Ogni persona può essere associata a diversi profili di abilitazione, in funzione di diverse situazioni e contingenze che possono verificarsi (es. emergenze, guardie, etc.). Il profilo di abilitazione secondo cui opera la persona è registrato al momento dell'accesso al sistema.

L'associazione di una persona fisica ad un profilo è effettuata da personale esplicitamente autorizzato (mediante un apposito profilo di abilitazione) e viene registrata.

Tenuto conto della possibile mobilità del personale, il totale assicura che in ogni momento le abilitazioni concesse ai singoli utenti siano relative alle sole unità operative/gruppi funzionali in cui i singoli prestano servizio.

Il titolare gestisce -preferibilmente in forma informatizzata- un "Registro complessivo dei profili di abilitazione" descrittivo dei profili definiti nei singoli sistemi informatizzati con la individuazione dei relativi privilegi e delle persone fisiche afferenti ai profili stessi e dei relativi periodi di abilitazione, mantenendo la storia delle abilitazioni precedenti.

Il titolare definisce una procedura per la disattivazione delle abilitazioni al momento del termine del rapporto di collaborazione e per la verifica periodica delle abilitazioni degli utenti, secondo i criteri previsti nella sezione "Riesame dei diritti di accesso degli utenti" al § 5.1.1 dell'Allegato C del documento "Linee guida di sicurezza nello sviluppo di applicazioni", Agenzia per l'Italia Digitale, ver. 1.0 del 21.11.2017, riportate nel seguito [13]:

> *I diritti di accesso degli utenti dovrebbero essere riesaminati regolarmente (al massimo ogni sei mesi) e dopo ogni cambiamento (es. cessazione del rapporto di lavoro, cambio di ruolo, di mansione, all'interno dell'organizzazione).*
> *Le autorizzazioni per i diritti di accesso privilegiati dovrebbero essere riesaminate ad intervalli più frequenti e gli eventuali cambiamenti tracciati.*
> *Per ogni cambiamento di privilegi deve esserne registrato il richiedente, l'approvatore e la motivazione. In caso di cessazione del rapporto di lavoro, sia di personale interno sia esterno, è necessario verificare i requisiti per la rimozione, o sospensione dei diritti di accesso al sistema/piattaforma.*
> *Tali diritti dovrebbero essere ridotti o rimossi prima della cessazione o della variazione del rapporto di lavoro, a seconda della valutazione di fattori di rischio come:*
> - *criticità delle informazioni cui si accedeva;*
> - *ruolo della persona,*
> - *motivazione della cessazione/cambiamento.*
>
> *Vanno previsti controlli o misure di sicurezza per limitare il rischio che:*

13 https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

- *in caso di licenziamento o fine contratto, dei dipendenti scontenti o degli utenti di terze parti esterne possano deliberatamente corrompere informazioni o commettere illeciti;*
- *in caso di persone dimissionarie o in uscita, esse possano essere tentate di recuperare/copiare informazioni per uso futuro.*

6.3.2 Situazioni particolari

a. Turnazione e/o emergenza

Come descritto in § 6.1.1.3.a, in alcuni contesti, a fronte di situazioni di turnazione e/o di emergenza, personale sanitario non afferente al Nucleo di Riferimento e quindi normalmente non abilitato (es. medico di guardia) deve poter accedere per visionare i dati del paziente per prendere decisioni ed attivare le funzionalità necessarie per eseguire attività mediche ed assistenziali nell'interesse del paziente stesso.

b. Richieste di informazioni e/o di pareri

Come descritto in § 6.1.1.3.b, in qualsiasi momento -anche al di fuori di contatti e senza limiti temporali- personale medico del titolare può ricevere dall'autorità giudiziaria, da altre strutture o singoli professionisti al momento impegnati nell'erogazione di servizi sanitari all'interessato o dall'interessato stesso, la motivata richiesta di dati personali e/o pareri per i quali sia necessario l'accesso a dati personali raccolti durante l'erogazione di servizi sanitari erogati in precedenza all'interessato.

c. Esportazioni massive di dati personali dai sistemi informatizzati

Le possibili soluzioni a queste esigenze sono dipendenti dalle caratteristiche dei sistemi informatizzati interessati, sono definite dall'organizzazione e vengono indicate nel "Registro dei sistemi informatizzati".

A solo titolo di esempio:

- per quanti riguarda il caso a., si può prevedere la definizione di un apposito profilo (es. "medico di guardia") e l'associazione a questo dell'utente interessato, effettuata -per il solo periodo di validità- da un ufficio centrale o da un componente autorizzato del Nucleo di riferimento o da un sistema informatico, oppure nell'accesso al sistema sotto la supervisione di un componente del Nucleo di riferimento, oppure l'integrazione con il sistema informatizzato di gestione del personale dal quale reperire automaticamente tali ruoli, etc..

- per quanto riguarda il caso b., si può prevedere la definizione di un apposito profilo associato agli utenti autorizzati che consenta di

accedere ai dati del paziente interessato e la specifica della motivazione al momento dell'accesso.

- per quanto riguarda il caso c., si può prevedere che le relative funzionalità siano associate a profili specifici assegnati a personale individualmente ed esplicitamente autorizzato.

Gli accessi effettuati in queste circostanze, se non desumibili ed evidenziabili tramite i log del sistema informatico interessato, sono registrati in un apposito registro centralizzato.

Secondo una periodicità definita dal titolare in funzione della criticità del settore, vengono effettuate verifiche sugli accessi effettuati secondo queste modalità per riscontrare eventuali incoerenze, registrandone le risultanze.

6.3.3 Attività eseguite senza l'utilizzo di sistemi informatizzati

Il titolare definisce procedure documentate che -per quanto possibile- regolamentino e permettano di tenere sotto controllo l'accesso ai dati personali secondo i criteri esposti anche per le attività eseguite mediante documenti cartacei, senza l'utilizzo di sistemi informatizzati.

7. Registri delle attività di trattamento

7.1 Obiettivi e contenuti

Per assicurare una visione organica e complessiva, i registri dei trattamenti sono organizzati in un documento unitario, strutturato secondo la classificazione delle finalità dei trattamenti stessi, come indicata nel § .... e contenente -per ogni trattamento- le informazioni prescritte dal Regolamento.

Considerato che ogni trattamento si articola in uno o più processi, organizzativi e/o sanitari, eseguiti con modalità, procedure e tecnologie diverse, per ogni trattamento sono individuati i processi relativi, specificando per ognuno di essi:

a) le eventuali procedure organizzative applicabili in relazione alla protezione dei dati personali;
b) le modalità di esecuzione, se manuale o supportata da sistemi informatizzati;
c) le principali tipologie di dati utilizzati, fermi restando i criteri di necessità ed accessibilità esposti al § 7.1;
d) il riferimento alle eventuali valutazioni di impatto effettuate sul trattamento in generale o sue singole attività;
e) in caso di attuazione mediante sistemi informatizzati, il riferimento alle relative sezioni del "Registro dei sistemi informatizzati" e del "Registro dei profili di abilitazione"

f) il riferimento ad eventuali iniziative evolutive, in corso o previste, circa le modalità e/o le tecnologie mediante le quali il processo è implementato.

7.2 Valutazione della liceità del trattamento

Preventivamente alla implementazione di un nuovo trattamento, classificabile secondo una delle tipologie b, c, d, e. del § 3.2.1, il titolare -per tramite del Comitato per la protezione dei dati personali- analizza e documenta le finalità e la liceità del trattamento previsto, in base alle condizioni espresse all'articolo 6 del Regolamento stesso.

Sotto il profilo metodologico, il fondamento di liceità deve essere identificato tenuto conto ed in ragione della finalità del trattamento.

Può verificarsi infatti che lo stesso set di dati venga raccolto e trattato (anche in tempi differenti) per finalità diverse (solo a titolo di esempio si pensi a dati raccolti e trattati per attività di diagnosi e cura, successivamente poi trattati per ricerca scientifica o studio epidemiologico).

Occorre quindi procedere come di seguito:

- identificare il set di dati sottoposti a una o più operazioni di trattamento
- identificare per tali dati la finalità di trattamento (art. 5, par 1, lett. b del Regolamento)
- identificare quindi il fondamento di liceità di quello specifico trattamento, attraverso l'analisi delle condizioni elencate all'art. 6 ed all'art. 9 del Regolamento

Sulla base di quanto formalizzato relativamente alle finalità del trattamento e verificato in termini di liceità, vengono poi derivati gli altri criteri secondo cui organizzare il trattamento nel rispetto dei principi di cui all'art. 5 del Regolamento, in particolare gli aspetti di minimizzazione, esattezza e conservazione (rispettivamente articolo 5 par 1 lettera c, d, e).

7.3 Modalità di tenuta

Il registro delle attività dei trattamenti è mantenuto preferibilmente in forma informatica ipertestuale per facilitare l'integrazione e l'accesso ai diversi documenti ed alle diverse informazioni referenziate.

8. Sicurezza

8.1 Sistemi informatizzati centralizzati, condivisi ed individuali

La classificazione dei sistemi informatizzati (inclusi i dispositivi medici) in termini di "centralizzato", "condiviso" ed "individuale" -secondo i criteri espressi nelle Definizioni- viene esplicitata nel "Registro dei sistemi informatizzati".

Considerata la maggiore criticità -per loro stessa natura anche dal punto di vista della dislocazione, protezione ed accessibilità- dei sistemi classificati come "condivisi" ed "individuali", il titolare definisce procedure specifiche per la gestione ed il monitoraggio degli stessi, con particolare riguardo a:

a) le modalità di registrazione e di accessibilità locale dei dati, che devono essere preferibilmente crittografati e non devono essere accessibili al di fuori delle procedure applicative se non a profili di utenza specifici, assegnati individualmente;
b) le modalità di backup;
c) il non utilizzo di dispositivi di registrazione dati removibili;
d) le modalità per un eventuale accesso remoto e comunicazione autonoma con l'esterno.

8.2 Identificazione

L'identificazione dell'utente e l'accesso alle procedure informatizzate è consentito a fronte di credenziali individuali, il più possibile gestite centralmente ed uniche per ogni utente per tutte le procedure dell'organizzazione.

Il titolare definisce una procedura per l'assegnazione delle credenziali che preveda l'identificazione ed il riconoscimento documentato della persona prima dell'assegnazione delle credenziali stesse.

L'anagrafica di tutti utenti abilitati ai sistemi informatici è gestita centralmente, e contiene, oltre ai dati identificativi dell'utente stesso, informazioni relative all'affiliazione dell'utente (dipendente o collaboratore dell'organizzazione del titolare, singolo professionista esterno, dipendente o collaboratore di altra struttura sanitaria cooperante nella cura ed assistenza del paziente, dipendente o collaboratore di un fornitore, etc.), il periodo di abilitazione. La disattivazione di un utente non comporta la cancellazione fisica dello stesso dall'archivio. L'accesso all'archivio degli utenti è riservato a personale autorizzato, mediante un apposito profilo di abilitazione.

La definizione delle credenziali e l'identificazione degli utenti nell'accesso al sistema è eseguita in accordo con quanto previsto al § 5.1.2 "Autenticazione" dell'Allegato C del documento "Linee guida di sicurezza nello sviluppo di applicazioni", Agenzia per l'Italia Digitale, ver. 1.0 del 21.11.2017 [14]:

Ove non già esistente, è obiettivo del titolare l'implementazione di un sistema unico cui facciano riferimento tutti i sistemi informatizzati dell'organizzazione per l'accettazione delle credenziali e l'identificazione dell'utente.

14 https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

La possibilità dei diversi sistemi di operare secondo credenziali individuali uniche e di identificare l'utente mediante un unico sistema centralizzato viene documentata nel "Registro dei sistemi informatizzati".

Le credenziali hanno il solo scopo di identificare l'utente e non comportano automaticamente alcun profilo di abilitazione, che deve essere esplicitamente associato ad ogni utenza, fra quelli previsti nel sistema acceduto.

8.3 Registrazione degli accessi e delle attività

E' obiettivo del titolare che:

a) tutti gli accessi ai sistemi informatici siano registrati in un log -il più possibile centralizzato-, all'inizio ed alla fine di ogni sessione;
b) le sessioni operative non possano rimanere attive a tempo indeterminato, al fine di limitare il rischio di accesso non autorizzato a stazioni di lavoro temporaneamente non presidiate.
   A questo scopo, in funzione delle caratteristiche e delle esigenze degli specifici contesti operativi, il titolare definisce un tempo massimo di inattività, al termine del quale il sistema deve richiedere all'utente una nuova identificazione con le proprie credenziali. Il tempo massimo di inattività stabilito per ogni sistema è definito nel "Registro dei sistemi informatizzati"
c) i sistemi informatizzati siano in grado di tenere traccia della data e dell'autore dell'ultima variazione di ogni record contenente dati personali e di mantenere in un log il dettaglio delle attività effettuate da ogni utente nel corso della sessione, con i dati acceduti e/o modificati.

Almeno per i sistemi informatizzati a supporto delle aree di maggior criticità e per i sistemi informatizzati accessibili dall'esterno dell'organizzazione da parte di utenti di altre organizzazioni e/o dal paziente stesso in un contesto di collaborazione territoriale, è impegno del titolare implementare queste funzionalità nelle nuove realizzazioni e di evolvere -ove non comporti uno sforzo sproporzionato- in questo senso i sistemi già esistenti.

Nel "Registro dei sistemi informatizzati" è evidenziata, per ogni sistema, la capacità di rispondere a questi requisiti ed è definito l'eventuale piano evolutivo.

8.4 Sicurezza e ripristino dei dati

Sia per fini di rispristino in caso di errori o incidenti, sia per poter ricostruire il contesto a fronte del quale sono state prese decisioni, è obiettivo del titolare mantenere traccia, nei sistemi informatizzati, della storia del valore assunto nel tempo da ogni singolo record contenente dati personali e di poter evidenziare i valori assunti dagli stessi nei diversi momenti insieme agli autori delle modifiche effettuate.

Almeno per i sistemi informatizzati a supporto delle aree di maggior criticità e per i sistemi informatizzati accessibili dall'esterno dell'organizzazione da parte

di utenti di altre organizzazioni e/o dal paziente stesso in un contesto di collaborazione territoriale, è impegno del titolare implementare queste funzionalità nelle nuove realizzazioni e di evolvere -ove non comporti uno sforzo sproporzionato- in questo senso i sistemi già esistenti.

Nel "Registro dei sistemi informatizzati" è evidenziata, per ogni sistema, la capacità di rispondere a questo requisito ed è definito l'eventuale piano evolutivo.

8.5 Psudonimizzazione

Quei trattamenti che comportino analisi massive e profilazione delle persone con finalità di prevenzione e ricerca, con la necessità di individuare l'interessato nel caso emergano situazioni di interesse per lo stesso sono effettuati in forma informatizzata adottando meccanismi di pseudonimizzazione, su archivi separati da quelli di produzione, privi dei dati identificativi della persona o con dati mascherati.

Il titolare definisce una procedura che preveda, per ogni trattamento, la documentazione dei dati di interesse da prelevare dai sistemi di produzione ed i meccanismi di eliminazione o mascheramento dei dati identificativi della persona, con particolare riguardo alla eventuale presenza dati non strutturati (testuali, immagini, etc.) che possano contenere informazioni identificative.

Per garantire la sicurezza e l'integrabilità di dati provenienti da sistemi diversi e prodotti da diversi fornitori, l'identificatore che, nell'ambito del processo di pseudonimizzazione, consente di risalire all'interessato è crittografato mediante un algoritmo basato su chiave asimmetrica di lunghezza minima 2048 bit.

L'eventuale identificazione dell'interessato nel caso in cui -in accordo con le finalità del trattamento- emergano aspetti per cui risulti necessario identificarlo e contattarlo nel suo interesse, viene effettuata mediante una procedura informatizzata:

a) che sia accessibile solo a persone individualmente autorizzate, per periodi di tempo non indefiniti;
b) che non consenta la visualizzazione o l'esportazione della chiave di decodifica;
c) che registri in un apposito registro -preferibilmente centralizzato- l'avvenuta identificazione dell'interessato e le motivazioni dell'identificazione stessa.

8.6 Ambienti di sviluppo, di test e di addestramento

Gli ambienti di sviluppo, di test e di addestramento necessari per l'evoluzione di sistemi esistenti e/o per l'implementazione di nuovi sistemi informatizzati si basano su dati completamente fittizi o -se prelevati dai sistemi di produzione- con i dati identificativi della persona mascherati, senza alcuna possibilità di risalire all'identità dell'interessato.

Il titolare definisce una procedura che preveda la documentazione di ogni ambiente, comprensiva dell'individuazione dei dati di interesse da prelevare dai sistemi di produzione e dei meccanismi mascheramento dei dati identificativi della persona, con particolare riguardo alla eventuale presenza dati non strutturati (testuali, immagini, etc.) che possano contenere informazioni identificative.

8.7 Infrastruttura tecnologica

Per la sicurezza dell'infrastruttura tecnologica, il titolare implementa, almeno al livello definito come "standard", le "Misure minime di sicurezza ICT per le pubbliche amministrazioni" definite nella circolare dell'Agenzia per l'Italia Digitale n. 2/2017 del 18 aprile 2017 [15].

E' possibile uno stato iniziale corrispondente al livello definito come "minimo", purché accompagnato da un piano evolutivo che porti al livello definito come "standard" nell'arco di 12 mesi.

Relativamente agli accessi dall'esterno mediante collegamenti protetti VPN (gestiti ed assegnati secondo quanto prescritto dal predetto documento), il titolare implementa un registro centralizzato e definisce una procedura di monitoraggio periodico degli accessi e delle attività effettuate attraverso tali collegamenti.

8.8 Sanificazione digitale

Il titolare definisce una procedura per la cancellazione sicura dei dati personali presenti su apparecchiature e dispositivi dismessi o consegnati a terzi, ad esempio per manutenzione.

8.9 Comunicazioni / invio di documentazione

8.9.1 APP e dispositivi usati in mobilità e forniti al paziente

"app" e dispositivi utilizzati in mobilità al di fuori dell'organizzazione (es. assistenza domiciliare) e/o forniti da parte dell'organizzazione al paziente per uso autonomo (es. telemedicina) prevedono la comunicazione mediante protocolli sicuri e crittografati e la registrazione dei dati direttamente ed esclusivamente su server gestiti dall'organizzazione.

8.9.2 Comunicazioni estemporanee fra operatori

Comunicazioni estemporanee contenenti informazioni relative allo stato di salute del paziente effettuate fra operatori sanitari e fra operatori sanitari e pazienti utilizzano strumenti di messaggistica basati crittografia "end-to-end".

8.9.3 Trasmissione di documentazione al paziente

15 https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

L'invio per modalità informatica di documentazione all'interessato (es. referti, prescrizioni, etc.) viene preferibilmente effettuata attraverso l'accesso dell'interessato ad un sistema informatizzato (per il quale valgono tutte le regole di abilitazione e sicurezza definite in questo codice) ed il conseguente prelievo della documentazione di interesse da parte dello stesso.

Qualora sia utilizzata la posta elettronica, i documenti trasmessi sono crittografati e/o protetti con password e la chiave di decodifica viene trasmessa all'interessato mediante una comunicazione separata, preferibilmente non di posta elettronica.

8.9.4 Posta elettronica

La posta elettronica implementata dall'organizzazione si basa su protocolli di comunicazione protetti, almeno il protocollo TLS.

8.10 Gestione dei documenti cartacei

Il titolare definisce una procedura per la gestione, consultazione, trasmissione e conservazione di documenti cartacei contenenti dati personali, che rispecchi -per quanto possibile- i criteri di abilitazione, redazione e sicurezza definiti in questo codice.

9. Valutazione d'impatto sulla protezione dei dati

9.1 Ambiti di applicazione

Obiettivo della valutazione di impatto è individuare se un trattamento o una attività all'interno di un trattamento presenta rischi per i diritti dell'interessato [16], con particolare riguardo alla liceità dell'utilizzo dei dati, ed ai rischi di diffusione e di accesso non autorizzato ai dati stessi.

Fermi restando i casi espressamente previsti dal Regolamento, il Comitato per la protezione dei dati analizza -preventivamente all'implementazione- la necessità di una valutazione d'impatto sulla protezione dei dati ogni qual volta si implementino nuovi trattamenti ed ogni qual volta vengano attivate nuove attività e/o variate le tecnologie e le procedure nell'ambito di trattamenti e/o attività già in essere basate su dati non anonimi e non psudonomizzati, con particolare riferimento alle attività finalizzate alla erogazione di servizi sanitari all'interessato.

La valutazione di impatto viene sempre effettuata nel caso di attività (nuove o variate in termini di procedure organizzative e/o tecnologie utilizzate) basate su

16 articolo 35.1 del Regolamento

dati non psudonomizzati e finalizzate all'erogazione di servizi sanitari, con finalità di prevenzione, cura o assistenza:

a) che siano articolate sul territorio e che prevedano la collaborazione di soggetti esterni all'organizzazione, incluso l'assistito;
b) che includano il monitoraggio continuo o periodico dell'assistito, mediante l'acquisizione di dati relativi al suo stato di salute e/o stili di vita e/o localizzazione geografica[17];
c) che richiedano l'acquisizione e/o l'utilizzo di dati genetici.

La decisione del Comitato circa l'effettuazione o meno della valutazione di impatto viene registrata.

9.2 Modalità di esecuzione

La valutazione d'impatto viene effettuata sotto la responsabilità e con il contributo di tutti i componenti del Comitato per la protezione dei dati, al fine di tener conto -oltre che di quanto previsto espressamente dal Regolamento- anche di altre componenti di rischio, quali quello clinico, gli aspetti organizzativi, le esigenze di formazione degli utenti ed eventuali limitazioni delle tecnologie disponibili.

Nell'ambito di quanto definito nel documento "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento 'possa presentare un rischio elevato' ai fini del regolamento (UE) 2016/679*" (WP 248 rev 01 [18]) la valutazione di impatto dedica particolare attenzione a:

a) le modalità di raccolta, condivisione e gestione di dati mediante documenti cartacei e comunicazioni verbali con l'interessato e/o i vari soggetti partecipanti al processo sanitario;
b) la rispondenza di tutti i componenti del trattamento/attività ai criteri di abilitazione e di sicurezza descritti ai § 7 e § 8 di questo codice;
c) la sicurezza dei meccanismi informatici di comunicazione, e di registrazione dati;
d) le caratteristiche e le modalità di funzionamento di eventuali dispositivi medici utilizzati per la rilevazione e la comunicazione dei dati;

Sulla base dell'esito della valutazione di impatto, il titolare può stabilire ed attuare misure specifiche per ridurre il rischio, fra le quali:

a) una informativa specifica nei confronti dell'interessato e l'eventuale richiesta di consenso esplicito da parte dello stesso;

[17] es. la localizzazione di pazienti affetti da malattie degenerative psichiche
[18] Gruppo di lavoro articolo 29 per la protezione dei dati, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

b) la definizione di procedure organizzative dedicate per la gestione di eventuali documenti cartacei connessi con lo specifico trattamento/attività;
c) l'implementazione di soluzioni tecnologiche in termini di registrazione, sicurezza, abilitazione e comunicazione più stringenti di quanto previsto in questo Codice di condotta;
d) la definizione di specifiche procedure per la formazione del personale coinvolto, ed anche dell'interessato qualora il trattamento implichi l'interazione con lo stesso nell'ambito di processi territoriali.

La valutazione di impatto, con le relative risultanze e le eventuali misure attuate, viene registrata nella documentazione del Sistema di gestione per la protezione dei dati personali e referenziata sia nel Registro dei trattamenti, che nel Registro dei sistemi informatizzati.

9.3 Riesami periodici

Nell'ambito dei riesami periodici previsti dal Sistema di gestione per la protezione dei dati personali sono riesaminate anche le valutazioni di impatto effettuate, al fine di verificarne la perdurante adeguatezza ed identificare eventuali ulteriori rischi.