**REGOLAMENTO SUL TRATTAMENTO DEI DATI PERSONALI**

**IN AMBITO SANITARIO E SOCIOSANITARIO**

**PREMESSA**

Le regole stabilite nel presente Regolamento devono essere applicate dai soggetti che trattano dati personali di natura particolare nell’Azienda Socio Sanitaria Territoriale di Lodi, di seguito “ASST”, nei confronti degli “utenti” del Servizio Sanitario e Sociosanitario, definiti anche “pazienti”, “cittadini” o “interessati”;

Il Regolamento contiene prescrizioni:

* per la gestione di dati particolari degli utenti per finalita’ di cura
* per l’esercizio dei diritti degli interessati.

Contiene inoltre in allegato il modulo di richiesta di autorizzazione per accesso, raccolta ed elaborazione dati aziendali per finalità di:

* elaborazione tesi di laurea, ricerca, relazione, pubblicazione
* presentazione in Convegni, Seminari, e Attività similari.

Scopo del presente Regolamento è quello di definire, in tutti i suddetti contesti, nel caso in cui l’Azienda operi in qualità di Titolare del trattamento dei dati dei soggetti interessati, le modalità di applicazione della normativa in tema di tutela e sicurezza dei dati personali, con particolare riferimento ai principi che la ispirano, ovvero:

* principio di liceità
* principio di trasparenza
* principi di correttezza, necessità e proporzionalità
* principio della limitazione della conservazione
* principi di riservatezza e d’integrità del dato.

Il Regolamento disciplina inoltre le modalità di raccolta e gestione del consenso alla costituzione del Dossier Sanitario Elettronico (DSE). Nel caso della ASST di Lodi, il Dossier Sanitario Elettronico è costituito dalla Cartella Clinica e Ambulatoriale (EMR) gestita tramite il sistema informatico Galileo©.

Il trattamento dei dati che non rispetta i principi e le modalità di seguito illustrati si configura come:

* violazione della disciplina vigente
* mancato rispetto delle disposizioni aziendali

con le conseguenze previste da leggi, CCNL e Regolamenti in materia disciplinare ed etico-comportamentale.

Il Regolamento verrà portato a conoscenza di:

* tutti i Responsabili del trattamento
* tutti i soggetti autorizzati al trattamento dei dati
* tutti gli amministratori di sistema, anche attraverso azioni formative dedicate.

# Poiché il presente Regolamento sostituisce la Procedura Privacy PR.46 (“Codice Privacy”)la relativa sarà modificata e adeguata a seguito dell’adozione dello stesso.

## PRESCRIZIONI PER LA GESTIONE DI DATI PARTICOLARI DEGLI UTENTI PER FINALITA’ DI CURA

1. **PRINCIPIO DI LICEITA’ DEL TRATTAMENTO**

La base giuridica che rende lecito il trattamento è la **finalità di cura,** ed in particolare l’esecuzione della prestazione richiesta dal paziente, qualificata come “compito del Servizio Sanitario Nazionale e dei soggetti operanti in ambito sanitario”.

Con riferimento ai trattamenti per **finalità di cura,** il Garante chiarisce che il professionista sanitario, proprio perché tenuto al segreto professionale, **non deve richiedere il consenso** del paziente per i trattamenti necessari alla prestazione sanitaria richiesta dall’interessato, ossia essenziali per il raggiungimento di finalità determinate ed esplicitamente connesse alla cura della salute, indipendentemente dal fatto che operi come libero professionista presso uno studio medico oppure all’interno di una struttura sanitaria pubblica o privata.

Deve però trattarsi delle prestazioni “necessarie”, essenziali per la cura della salute nel caso specifico e/o per garantire la continuità dell’assistenza sanitaria o sociale.

Per le prestazioni non strettamente necessarie – ancorchè legittimamente svolte – sarà necessario il consenso, oppure che vi sia oggettiva evidenza di:

* salvaguardia degli interessi vitali dell’interessato o di un’altra persona fisica
* esecuzione di un compito di interesse pubblico, tra cui:
  + attività amministrative e certificatorie, correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d’organo e di tessuto, nonché alle trasfusioni di sangue umano
  + compiti del Servizio sanitario nazionale e dei soggetti operanti in ambito sanitario
  + programmazione, gestione, controllo e valutazione dell’assistenza sanitaria
  + vigilanza sulle sperimentazioni e farmacovigilanza
  + tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili.

Tra i trattamenti in ambito sanitario – di interesse di questa Azienda, che invece richiedono il consenso espresso dell’interessato, il Garante segnala:

* i trattamenti connessi all’utilizzo di app mediche
* l’apertura del Dossier Sanitario Elettronico (DSE)
* l’apertura del Fascicolo Sanitario Elettronico (FSE).

Ai fini dell’applicazione del presente Regolamento, per “CONSENSO” si intende pertanto:

* il consenso al trattamento dei dati, ove necessario;
* il consenso alla costituzione del DSE, sempre obbligatorio;
* il consenso alla comunicazione a terzi dei dati, sempre obbligatorio.

**IN PARTICOLARE, IL CONSENSO PER GLI OPERATORI CHE UTILIZZANO I SOFTWARE “GALILEO” , “CAMELIA” E APPLICATIVI CON FUNZIONI ANALOGHE**

Si precisa prioritariamente che:

* l’informativa ed il consenso al trattamento dei dati personali possono essere resi ed acquisiti successivamente alla prestazione, ma senza ritardo, **in caso di emergenza sanitaria o di igiene pubblica** per la quale la competente Autorità ha adottato un’ordinanza contingibile ed urgente, ai sensi dell’art.117 del D. Lgs. n° 112/1998;
* l’informativa ed il consenso possono essere resi ed acquisiti successivamente alla prestazione, ma senza ritardo, in caso di:

1. **presenza di impedimenti fisici, incapacità di agire o incapacità di intendere o di volere dell’interessato,** quando non è possibile acquisire il consenso da chi esercita legalmente la potestà ovvero da un prossimo congiunto, da un familiare, da un convivente o in loro assenza dal responsabile della struttura presso cui dimora l’interessato;
2. **rischio grave, imminente ed irreparabile per la** salute dell’interessato;
3. prestazione medica che può essere pregiudicata dalla acquisizione preventiva del consenso in termini di **tempestività o efficacia.**

Nel caso di **pazienti minorenni**, il consenso deve essere obbligatoriamente firmato da ENTRAMBI I GENITORI o da chi esercita legalmente la potestà. Dopo il raggiungimento della maggiore età, il consenso deve essere nuovamente richiesto e firmato dall’interessato.

E’ fatto **assoluto divieto** agli operatori di tutte le professioni di visionare impropriamente dati di pazienti/utenti**.** Nel sistema resta traccia di tutti gli accessi effettuati dal personale. Saranno effettuati dei controlli in tal senso.

**Come è registrato il consenso degli interessati in GALILEO**

Il software consente di registrare con un flag solo il consenso per l’attivazione del Dossier sanitario. Gli operatori autorizzati possono registrare queste tipologie di consenso:

* **Non Espresso**: valore utilizzato per indicare l’assenza di alcuna indicazione di consenso. L’assenza di espressione viene trattata come negazione del consenso.
* **Si, creazione del Dossier anche per lo storico:** valore utilizzato per consentire la creazione e consultazione del Dossier di tutti gli eventi che riguardano il paziente e presenti nel data base.
* **Si, creazione del Dossier da oggi in avanti:** valore utilizzato per consentire la creazione e consultazione del Dossier di tutti eventi che riguardano il paziente, successivi alla registrazione del consenso.
* **No, nessuna creazione del Dossier:** valore utilizzato per non consentire la creazione e la consultazione del Dossier.

Il flag che consente la registrazione dei consensi non è obbligatorio; questa registrazione è volontaria e consente di attivare l’accesso al dato storico del paziente. Questa attività è oggetto di tracciamento all’interno del log.

In occasione di ogni ricovero, il paziente è tenuto a sottoscrivere il modulo di consenso che viene poi allegato alla cartella clinica.

Ferme restando eventuali ulteriori disposizioni, si riportano i percorsi stabiliti ad oggi.

**UTENTE OSPEDALIERO**

**Acquisizione del consenso:** il diretto interessato ad oggi presta il consenso al trattamento dati, alla costituzione del DSE e alla comunicazione a terzi compilando e firmando il relativo modulo [Pr.46 Mod. 1]; l’Operatore annoterà il consenso alla costituzione del DSE, se non ancora registrato, nell’apposito campo del sistema informativo (CCE – Galileo).

Il consenso deve essere acquisito ad ogni singolo ricovero. Tale consenso è considerato valido per la pluralità delle prestazioni erogate, dalle distinte Unità Operative di quest’Azienda, per trattamenti clinici e strumentali, a valenza sia diagnostica sia terapeutica, necessari per l’erogazione della prestazione, anche presso altre Aziende sanitarie. Tale consenso può essere in ogni momento rettificato o revocato da parte dell’Interessato. Il modulo diventa parte integrante di tutta la documentazione che costituisce la cartella clinica.

**UTENTE AMBULATORIALE**

**Acquisizione del consenso:** il diretto interessato ad oggi presta il consenso al trattamento dati in forma orale; l’Operatore annoterà l’avvenuto consenso nell’apposito campo del sistema informativo (CUP – Camelia). Il consenso verrà richiesto all’atto della prenotazione/accettazione amministrativa.

Sul modello cartaceo di prenotazione/accettazione comparirà la dicitura che attesta l’avvenuta acquisizione del consenso.

Nel caso di **prestazioni ambulatoriali cicliche**, il consenso viene acquisito una sola volta, è considerato valido per la pluralità delle prestazioni erogate e diventa parte integrante di tutta la documentazione che costituisce la cartella ambulatoriale [ PR.46 Mod. 3]

Nel caso di accesso ad una prestazione medica ambulatoriale, es. visita specialistica, il personale sanitario può raccogliere anche il consenso per la costituzione del Dossier Sanitario Elettronico (DSE), nel caso in cui non sia ancora stato espresso.

**UTENTE DI PRONTO SOCCORSO**

**Acquisizione del consenso**: il diretto interessato ad oggi presta il consenso compilando e firmando la formula di consenso riportata all’interno del foglio di Triage.

**UTENTE AMBULATORIALE AREA SOCIOSANITARIA**

**Acquisizione del consenso:** il diretto interessato ad oggi presta il consenso compilando e firmando il relativo modulo [Pr.46 – Mod. 5].

Il consenso viene acquisito all’apertura della cartella e vale per tutti gli accessi successivi, sia che si tratti di percorsi più complessi, che di mono prestazioni per trattamenti clinici e strumentali, a valenza sia diagnostica sia terapeutica, necessari per l’erogazione della prestazione. Tale consenso può essere in ogni momento rettificato o revocato da parte dell’Interessato.

Il modulo diventa parte integrante di tutta la documentazione che costituisce la cartella ambulatoriale.

**UTENTE SERVIZIO SANITA’ PENITENZARIA**

Acquisizione del consenso: il diretto interessato ad oggi presta il consenso compilando e firmando il relativo modulo [Pr.46 – Mod. 4] che sarà conservato nel fascicolo dell’utente.

**Raccolta del Consenso per il Fascicolo Sanitario Elettronico**

I documenti clinici elettronici (DCE) quali: lettere di dimissione, verbali di Pronto Soccorso, referti ambulatoriali o di diagnostica strumentale, sono sottoposti a firma digitale da parte del medico refertante ed archiviati in un’apposita piattaforma (EPR) facente parte del sistema CRS-SISS di Regione Lombardia.

La presenza di questi documenti viene notificata ai sistemi centrali di Regione Lombardia per la costituzione del Fascicolo Sanitario Elettronico (FSE). L’inserimento dei documenti clinici nel fascicolo FSE è subordinato all’espressione di un apposito consenso da parte del cittadino, in assenza del quale nessun dato risulta visibile all’interno del fascicolo FSE.

Le modalità di espressione e raccolta del consenso alla costituzione del FSE sono regolamentate da apposite procedure definite da Regione Lombardia accessibile sul sito istituzionale www.crs.regione.lombardia.it a cui si rimanda per ogni ulteriore dettaglio.

Conviene qui ricordare che la raccolta del consenso alla costituzione del FSE può essere effettuata da qualunque struttura sanitaria lombarda integrata con la rete CRS-SISS ed in particolare per l’ASST di Lodi presso i punti di Scelta e revoca del medico e presso gli Uffici di accoglienza.

1. **PRINCIPIO DI TRASPARENZA**

Il principio di trasparenza trova il suo principale strumento nell’**Informativa.**

L’informativa è lo strumento che rende esplicita e trasparente la gestione delle informazioni di carattere personale e sensibile degli interessati ed in tal modo consente agli stessi soggetti di prendere parte attiva alla difesa dei propri diritti nell’ambito della protezione dei dati personali.

Per questo motivo l’ASST informa preventivamente l’interessato tramite un’idonea informativa che contiene:

* le finalità e le modalità del trattamento dei dati;
* la base giuridica del trattamento e quindi la natura obbligatoria o meno del conferimento dei dati;
* le conseguenze di un eventuale rifiuto;
* i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possonovenirne a conoscenza;
* il periodo di conservazione dei dati o, se non è possibile, i criteri utilizzati per determinare tale periodo;
* qualora i dati non siano raccolti presso l’interessato, tutte le informazioni possibili sulla loro origine;
* l’esistenza di un processo decisionale automatizzato o di attività di profilazione;
* l’eventuale trasferimento a un Paese terzo o a un’organizzazione internazionale;
* i diritti dell’interessato;
* in particolare, il diritto di proporre reclamo a un’Autorità di controllo o giudiziaria;
* gli estremi identificativi del Titolare, del Responsabile del trattamento e del Responsabile della protezione dei dati (DPO).

L’ASST ha predisposto e pubblicato sul proprio sito, sulla scorta dei criteri elencati:

* l’informativa generale
* informative c.d. “stratificate”, ossia declinate in relazione al concreto ambito di attività .

L’Informativa per il trattamento dei dati personali e sensibili, generale o stratificata, è consegnata agli utenti e/o esposta in maniera visibile nei diversi punti di accesso alle strutture (stanze di degenza, punti di accettazione ambulatoriale, sale d’aspetto, CUP, reparti, uffici etc).

L’informativa deve essere inoltre fornita al momento della prenotazione/accettazione amministrativa o comunque prima dell’erogazione della prestazione sanitaria o sociosanitaria; per i servizi ad accesso diretto la consegna avviene al primo accesso al Servizio.

1. **PRINCIPIO DI CORRETTEZZA, NECESSITÀ E PROPORZIONALITA’**

Il trattamento dei dati personali avviene per finalità specifiche, esplicite e legittime, dettagliate ed esplicitate nell'informativa consegnata all'interessato.

Sono oggetto dei trattamenti i dati di utenti, pazienti e dei genitori/tutori/familiari con le modalità e per le finalità chiarite nell’informativa.

I dati degli interessati potranno essere resi accessibili, sempre e soltanto per le finalità dichiarate,a:

* dipendenti e collaboratori del Titolare coinvolti nel suo percorso di cura, nella loro qualità di Autorizzati e/o Responsabili interni del trattamento e/o Amministratori di sistema;
* Società terze quali: società informatiche per manutenzione dei software o Organizzazioni/Specialisti nella loro qualità di Responsabili esterni del trattamento:
* Organismi – ispettivi, di controllo, di riferimento - di Regione Lombardia e Ministero della Salute in qualità di Titolari autonomi del Trattamento.

La raccolta dei dati del paziente/utente può avvenire in tre momenti diversi:

* in fase di TRIAGE, qualora lo stesso transiti dal pronto Soccorso
* in fase di ACCETTAZIONE in reparto o nel Servizio da parte del personale autorizzato;
* tramite CUP per la prenotazione di visite ambulatoriali o esami.

Per alcune tipologie di visite e/o esami sono predisposti opportuni percorsi che non prevedono la prenotazione al CUP e che afferiscono direttamente al personale di reparto/Servizio.

Per verificare se i dati sono esatti e aggiornati, vengono condotti controlli sulla correttezza dei dati anagrafici del paziente.

La prima e fondamentale fase è l’identificazione.

Può essere svolta tramite ricerca su Anagrafica locale (del singolo applicativo), su Anagrafica aziendale, su Anagrafica regionale, utilizzando chiavi di ricerca quali nome, cognome, data di nascita, sesso.

È anche possibile utilizzare la Tessera Sanitaria del cittadino per l’acquisizione in modo automatico dei dati anagrafici, riducendo così il rischio di errore in fase di ricerca.

L’uso della Tessera Sanitaria in fase di identificazione del paziente permette infatti una selezione più sicura del soggetto ed evita errori dovuti a casi di omonimia. E’ necessario anche il controllo di un documento di riconoscimento.

La correttezza dei dati registrati è assicurata attraverso il controllo dei documenti che compongono la cartella clinica o ambulatoriale. Il personale autorizzato è esperto e formato periodicamente.

Una ulteriore fase di controllo viene effettuata in reparto/Servizio attraverso il contatto e lo scambio di informazioni con il paziente stesso o i suoi familiari, che possono evidenziare inaccuratezze dei dati anagrafici registrati.

Inoltre, i flussi informativi con Regione Lombardia possono ulteriormente evidenziare, anche se in modalità retroattiva, eventuali anomalie relative alla correttezza formale dei dati anagrafici.

1. **PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE**

Il Titolare tratterà i dati personali per il tempo necessario per adempiere al processo di cura.

In generale i dati personali saranno conservati sul data base di Galileo per un tempo indefinito al fine di consentire un percorso di cura non limitato al singolo episodio e consentire una valutazione clinica più completa.

Verrà valutato caso per caso quali sono i dati storici per cui non sussiste più la necessità/opportunità di mantenimento; in questi casi si procederà con una cancellazione selettiva e manuale dei dati presenti nel DSE.

La necessità di conservare un dato clinico risponde a diversi tipi di esigenze, tra cui:

* Aspetti giuridici per fini di autotutela piuttosto che di esibizione a richiesta dell’autorità giudiziaria;
* Aspetti clinici ai fini di un migliore processo di cura a fronte di una più completa visibilità dei precedenti storici del paziente;
* Aspetti legati ad attività di tipo statistico/epidemiologico.

In assenza di una norma precisa che stabilisca a priori il tempo massimo di conservazione per ogni tipo di documento clinico, l’unico criterio che può essere adottato per definire il periodo di conservazione più adeguato è quello basato su una comparazione tra tempi minimi di conservazione obbligatori, utilità del dato, non eccedenza nell’uso dei dati clinici.

1. **PRINCIPIO DI RISERVATEZZA**

I **medici e i professionisti sanitari e sociosanitari**, ciascuno secondo le competenze specifiche e previste dalla normativa vigente, hanno accesso alle informazioni sullo stato di salute del paziente/utente.

In GALILEO, avranno accesso alle seguenti schede della cartella informatizzata del paziente:

* Anamnesi familiare, remota;
* Allergie, anamnesi fisiologica;
* Problemi e Piano di Cura
* Richieste, Eventi, Codifica, Documenti e Firma documenti

In linea generale tali figure possono consultare solo le informazioni relative alle prestazioni svolte e alla condizione clinica dei pazienti del proprio reparto. Ai sensi del Provvedimento del 4 Giugno 2015 i medici e infermieri hanno infatti a disposizione solo le informazioni rese in quel momento dal paziente per l’intera durata della degenza nel proprio reparto e nel mese successivo alla dimissione.

Solo nel caso in cui l’utente abbia espresso il consenso alla creazione del Dossier Sanitario, il medico e l’infermiere possono consultare l’intero fascicolo, sempre per la durata della degenza e sino a un mese dopo la dimissione.

Il **medico legale** e gli s**pecialisti** incaricati dei controlli, anche epidemiologici, sono abilitati a consultare tutte le schede di Galileo e possono avere accesso anche agli episodi oggetto di oscuramento e anonimizzazione in caso di controversie legali con l’utenza (il medico legale) e le **indagini epidemiologiche (gli specialisti).**

1. **PRINCIPIO DI INTEGRITA’ DEL DATO**

La cartella informatizzata, una volta stampata, viene depositata nello studio dei medici di reparto e viene consegnata al coordinatore infermieristico alla dimissione del paziente, che ne verifica la completezza. L’Ufficio cartelle cliniche ritira le cartelle depositate e ne verifica la completezza secondo gli standard di accreditamento regionale prima di inviare la documentazione al Fornitore incaricato dell’opportuna archiviazione.

Per le cartelle ambulatoriali esistono similari sistemi di controllo e archiviazione.

**GESTIONE DEI RECLAMI PRIVACY E DELL’ESERCIZIO DEI DIRITTI DEGLI INTERESSATI**

Le regole stabilite dal presente Regolamento sono applicate dalla UOS attuazione normativa sulla riservatezza dei dati personali e dalle funzioni della ASST di Lodi che accolgono reclami – nella fattispecie, in tema di privacy - e richieste di esercizio di un diritto previsto dal Regolamento da parte degli interessati (pazienti e utenti, dipendenti e collaboratori a qualsiasi titolo) e che gestiscono questa materia in ottemperanza ai disposti del Regolamento UE 679/16 e del D. Lgs. 196/2003, come modificato dal D. Lgs. 101/2018.

Si riportano di seguito le seguenti definizioni, esemplificative degli eventi che potranno essere evitati con il rispetto delle disposizioni regolamentari.

|  |  |
| --- | --- |
| INCIDENTE | Relativamente alla sicurezza delle informazioni, uno o più eventi non voluti o inaspettati che hanno una significativa probabilità di compromettere la normale attività e minacciare la sicurezza delle informazioni |
| DATA BREACH | Effetto di un evento o di azione colposa / fraudolenta compiuta da un soggetto, che può compromettere o ha compromesso diritti e libertà delle persone fisiche interessate al trattamento |

# *GESTIONE DEL RECLAMO*

La gestione del reclamo in tema di privacy consente la gestione dei seguenti rischi:

* malcontento dell’interessato in presenza di una situazione che gli appare lesiva del suo diritto a mantenere riservate informazioni e dati che lo riguardano
* incidenti non rilevati dal personale interno
* eventuali comportamenti non conformi da parte del personale.

La sequenza delle fasi di gestione di un reclamo in materia di dati personali si configura come segue:

**FASE 1 – RICEZIONE DEL RECLAMO**

Il reclamo proveniente da un interessato può pervenire ad ASST Lodi:

1. tramite email, alla casella che fa riferimento all’URP, utilizzando il modello scaricabile dal sito web;
2. tramite presentazione diretta allo sportello URP di uno scritto (non necessariamente attraverso il modulo scaricabile dal web)
3. tramite lettera indirizzata ad ASST Lodi, che verrà consegnata all’URP e trasmessa da questo Ufficio al Protocollo aziendale;
4. verbalmente presso l’URP, che provvede ad identificare il reclamante ed a registrarne con puntualità le indicazioni;
5. tramite comunicazione di un avvocato che presenta via PEC il reclamo in nome e per conto dell’interessato, suo assistito;
6. tramite una PEC in arrivo direttamente dall’Ufficio del Garante che segnala l’apertura del procedimento (trasmessa all’attenzione del DPO).

Il personale dell’URP verifica se la natura del reclamo attiene alla protezione dei dati personali; nei casi dubbi si avvale del supporto dell’UOS Attuazione normativa sulla riservatezza dei dati personali per identificare se la natura del reclamo stesso è ascrivibile alla sfera della privacy.

Il DPO viene sempre messo a conoscenza dell’esistenza di un reclamo in tema di privacy.

**FASE 2 - PRESA IN CARICO DEL RECLAMO**

Dopo aver ricevuto il reclamo, ASST Lodi si attiva per svolgere le necessarie valutazioni di merito:

* nei casi da 1 a 4 della precedente Fase 1, l’URP trasmette la richiesta alla UOS Attuazione normativa sulla sicurezza dei dati personali, che fornisce le indicazioni per la risposta.
* nei casi 5 e 6, viceversa, sarà direttamente il DPO ad occuparsi di valutare le richieste in arrivo dal Garante o dal legale dell’interessato, identificando le opportune azioni da porre in essere. In particolare, valuterà se il reclamo sottenda all’accadimento di un incidente: in caso positivo, e comunque quando previsto, attiverà il Nucleo Data Breach della ASST Lodi che definirà ed applicherà le necessarie azioni in applicazione del REGOLAMENTO INCIDENTI, viceversa si preoccuperà più semplicemente di dare corso alle azioni definite in precedenza nel medesimo REGOLAMENTO.

**FASE 3 – FEEDBACK ALL’INTERESSATO**

A chiusura del presente percorso, la UOS suddetta comunicherà la risposta all’interessato in modo formale. La risposta verrà formulata in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, come per tutti gli altri riscontri forniti dalla UOS.

**FASE 4 – ARCHIVIAZIONE, RIESAME E MIGLIORAMENTO**

Una volta chiusi, i reclami inerenti la privacy vengono archiviati presso la UOS, che provvede a mantenerne aggiornato l’elenco.

Almeno una volta l’anno, il DPO riesamina i reclami ricevuti nel periodo precedente e sulla base dei dati che ne ricava definisce le eventuali misure di miglioramento da applicare: in tal caso, predispone un piano di attuazione di tali misure definendone gli obiettivi, le responsabilità, le risorse, i tempi di completamento. Il DPO monitora e verifica gli avanzamenti, valutando, al termine delle attività, l’efficacia di tali azioni.

## *RICHIESTE DI ESERCIZIO DEI DIRITTI PRIVACY*

Il percorso che segue consente di gestire i seguenti **rischi:**

* perdita di controllo del flusso dei propri dati da parte dell’interessato (accesso)
* trattamento di dati inesatti o incompleti (rettifica)
* conservazione di dati non più utili allo scopo per cui erano stati raccolti e per questo anche potenzialmente dannosi per la persona interessata (cancellazione; oblio)
* trattamento non consentito di dati o non conforme alla finalità della raccolta (opposizione)
* danno emergente o lucro cessante per impossibilità di trasferimento dell’insieme dei dati da un titolare ad un altro (portabilità)
* impossibilità per l’interessato di esercitare i propri diritti in sede giudiziaria (limitazione)

I diritti esercitabili dagli interessati sono i seguenti:

1. **IL DIRITTO DI ACCESSO**

La persona i cui dati sono oggetto di trattamento ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati e quali ne siano le caratteristiche.

In ambito “GALILEO”, qualora richiesto dall’interessato, Galileo consente l’esportazione dell’intera cartella clinica (master index e assemblato di tutti i documenti in formato .pdf).

Previo consenso dell’interessato (come già precisato), può essere attivato il Fascicolo Sanitario Elettronico che consente l’accesso al cittadino di documenti di tipo sanitario in un formato di uso comune.

**2. IL DIRITTO DI RETTIFICA**

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

In ambito “GALILEO”, la rettifica di dati registrati in modo erroneo può essere evidenziata direttamente al personale di reparto che effettuerà le verifiche e le correzioni necessarie, anche avvalendosi del supporto del Sistema Informativo.

A episodio di ricovero già chiuso, l’utente può rivolgersi agli sportelli URP per richiedere una rettifica dei dati e presentando idonea documentazione a supporto. L’ufficio URP provvederà a coinvolgere i servizi aziendali necessari per le opportune verifiche e correzioni.

**3. IL DIRITTO DI CANCELLAZIONE (OBLIO)**

La persona i cui dati sono oggetto di trattamento ha diritto, a certe condizioni, di ottenere dal titolare del trattamento la cancellazione dei dati personali che la riguardano senza ingiustificato ritardo e di conseguenza il titolare del trattamento, senza ingiustificato ritardo, ha l'obbligo di cancellare i dati personali.

1. **OSCURAMENTO IN AMBITO DOSSIER SANITARIO ELETTRONICO**

In ambito “GALILEO”, i pazienti attraverso la compilazione di un modulo (Pr.46 - Mod. 2 Richiesta oscuramento) hanno la possibilità di richiedere la limitazione all’accesso da parte del personale medico ad uno specifico evento del loro Dossier sanitario. Questa attività di “oscuramento” produce l’invisibilità completa di un episodio clinico.

Il software Galileo ha inoltre una funzione che consente il congelamento dell’intero fascicolo sanitario in caso di richiesta di blocco da parte dell’Autorità Giudiziaria.

Cosa può essere oscurato:

* l’intero DSE, attraverso la revoca del consenso
* un singolo episodio all’interno del DSE
* un documento clinico nel FSE (dal portale regionale)

Viene di seguito descritta – per ogni tipologia di utente - la modalità di raccolta della richiesta di oscuramento dei dati sanitari ai fini della visibilità all’interno del Dossier sanitario elettronico.

**Oscuramento dei dati sanitari in caso di utente ospedaliero:** nel caso di richiesta da parte del paziente di oscuramento dei dati sanitari per quello specifico evento, l’Operatore farà firmare la modulistica di richiesta [Pr.46 – Mod. 2], che sarà conservata insieme al modulo di consenso in cartella clinica e sarà inviata in copia all’Ufficio Relazioni con il Pubblico che provvederà ad inoltrarlo al SIA per gli adeguamenti informatici.

**Oscuramento dei dati sanitari per utente ambulatoriale:** nel caso di richiesta da parte del paziente di oscuramento dei dati sanitari per uno specifico evento, l’Operatore farà firmare la modulistica di richiesta [Pr.46 – Mod. 2] che sarà conservata nella cartella ambulatoriale e sarà inviata in copia all’Ufficio Relazioni con il Pubblico per gli adeguamenti informatici.

La richiesta di oscuramento può essere raccolta in fase di prenotazione/accettazione o successivamente presso l’ambulatorio.

**Oscuramento dei dati sanitari per utenti di Pronto Soccorso:** nel caso di richiesta da parte del paziente di oscuramento dei dati sanitari per quello specifico evento, l’Operatore farà firmare la modulistica di richiesta [Pr.46 – Mod. 2] che sarà conservata insieme al foglio di triage e sarà inviata in copia all’Ufficio Relazioni con il Pubblico per gli adeguamenti informatici.

Per i ricoveri d’urgenza (pazienti ricoverati dal Pronto Soccorso) gli adempimenti in tema di privacy (in particolare l’acquisizione del consenso) saranno di competenza delle Unità Operative di destinazione.

**Oscuramento dei dati sanitari per utente ambulatoriale area socio-sanitaria:** nel caso di richiesta da parte del paziente di oscuramento dei dati sanitari per quello specifico evento, l’Operatore farà firmare la modulistica di richiesta [Pr.46-Mod.2], che sarà conservata insieme al modulo di consenso nella cartella ambulatoriale e sarà inviata in copia all’Ufficio Relazioni con il Pubblico per gli adempimenti conseguenti.

**Oscuramento dei dati sanitari per utente sanità penitenziaria:** nel caso di richiesta da parte del paziente di oscuramento dei dati sanitari per quello specifico evento, l’Operatore farà firmare la modulistica di richiesta [Pr.46-Mod.2], che sarà conservata insieme al modulo di consenso nel fascicolo dell’utente e sarà inviata in copia all’Ufficio Relazioni con il Pubblico per gli adempimenti conseguenti.

**5. IL DIRITTO DI LIMITAZIONE**

La «limitazione di trattamento» è il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento nell’immediato o in futuro. La limitazione consiste, a determinate condizioni, nell’impedire qualsiasi tipo di operazione sui dati contrassegnati ad esclusione della conservazione.

**6. IL DIRITTO ALLA PORTABILITA’**

La persona i cui dati sono oggetto di trattamento ha diritto, a certe condizioni, di riceverli in un formato strutturato, di uso comune e leggibile da dispositivo automatico e ha diritto di trasmetterli ad un altro titolare se il trattamento si basava sul consenso oppure era effettuato con mezzi automatizzati.

**7. IL DIRITTO DI OPPOSIZIONE**

La persona i cui dati sono oggetto di trattamento ha diritto, a certe condizioni, di opporsi a questo trattamento a meno che il titolare del trattamento dimostri l’esistenza di motivi legittimi cogenti prevalenti.

ASST Lodi gestisce le richieste di esercizio dei diritti in tema di dati personali con le modalità descritte di seguito.

**FASE 1 – RICHIESTA**

L’interessato richiede di esercitare i suoi diritti in materia di privacy in tre diversi modi:

* tramite domanda, orale o scritta, rivolta all’URP
* attraverso il modulo reso disponibile sul sito web di ASST Lodi, presentato direttamente o tramite email
* tramite un difensore (previa apposita procura o delega che va allegata all’istanza).

In questa fase, è compito del personale autorizzato dell’URP accogliere le richieste e coinvolgere UOS Attuazione normativa sulla riservatezza dei dati personali per interpretare i bisogni dell’interessato, guidandolo all’occorrenza nella compilazione del Modello per l’esercizio dei diritti. La richiesta sarà successivamente trasmessa al Protocollo e presa in carico dalla UOS stessa.

**FASE 2 – ISRUTTORIA**

In caso di richiesta di esercizio dei diritti il titolare è tenuto a dare riscontro entro 30 giorni dalla data di inoltro con possibilità di ulteriori 30 giorni di tempo nel caso in cui la risposta sia problematica e che in ogni caso entro il 30 esimo giorno deve essere data comunicazione scritta delle motivazioni del ritardo.

L’URP trasmette la richiesta alla UOS Attuazione normativa sulla riservatezza dei dati personali che, con il supporto del DPO, verifica che:

* la richiesta sia stata formulata liberamente e senza costrizioni;
* salvo l'esistenza di giustificati motivi, la stessa richiesta non sia già stata presentata con intervallo di tempo inferiore ai 30 giorni;
* l’identità del richiedente sia effettivamente nota in ASST Lodi; per fare questo si basa su:
  1. atti ed anagrafiche
  2. documenti disponibili
  3. esibizione o allegazione di copia di un documento di riconoscimento.

La richiesta della persona interessata può essere soddisfatta anche qualora questa dovesse esercitare i propri diritti attraverso delega o procura scritta a persona fisica, enti, associazioni od organismi. Il difensore/delegato che agisce per conto della persona interessata deve esibire o allegare copia della procura, oppure della delega sottoscritta dall’interessato e presentata unitamente a fotocopia non autenticata di un documento di riconoscimento dell'interessato stesso.

E’ possibile richiedere informazioni anche per conto di un defunto solo se si dimostra che vi sia un interesse personale o che ciò avvenga nell’interesse del deceduto o per ragioni familiari meritevoli di protezione.

**FASE 3 – FEEDBACK ALL’INTERESSATO**

L’UOS Attuazione normativa sulla riservatezza dei dati personali formula una risposta scritta che, a seconda delle specifiche situazioni, accoglie totalmente o parzialmente la richiesta. La risposta verrà formulata in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

L’UOS Attuazione normativa sulla riservatezza dei dati personali ha la responsabilità di farla pervenire all’interessato attraverso tre possibili modalità:

* per iscritto, attraverso un documento cartaceo (es. lettera raccomandata) oppure con altri mezzi (CD; DVD) inclusi mezzi elettronici (email, PEC);
* oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato (in questo caso il dipendente autorizzato a trattare la pratica ne dovrà prendere sinteticamente nota in un registro);
* con semplice presa di visione delle informazioni attraverso strumenti elettronici, purché la comprensione sia agevole, tenuto conto della quantità e qualità delle informazioni.

L’ UOS Attuazione normativa sulla riservatezza dei dati personali informerà l’URP dell’esito dell’istruttoria e invierà per conoscenza all’ URP la risposta formulata all’interessato. L’UOS Attuazione normativa sulla riservatezza dei dati personali rilascia le informazioni richieste a titolo gratuito. Se le richieste dell'interessato sono manifestamente infondate o eccessive (ripetitive), su istruzione del Titolare può comunicare all’interessato la necessità di addebitare un contributo spese ragionevole (tenendo conto dei costi amministrativi sostenuti per fornire le informazioni, la comunicazione o per intraprendere l'azione richiesta) oppure può legittimamente rifiutarsi di soddisfare la richiesta.

**FASE 4 – ARCHIVIAZIONE, RIESAME E MIGLIORAMENTO**

Una volta chiuse, le richieste di esercizio dei diritti privacy vengono archiviate presso UOS Attuazione normativa sulla riservatezza dei dati personali, che provvede a mantenerne aggiornato l’elenco.

Almeno una volta l’anno, il DPO riesamina le richieste ricevute nel periodo precedente e sulla base dei dati che ne ricava definisce le eventuali misure di miglioramento da applicare: in tal caso, predispone un piano di attuazione di tali misure definendone gli obiettivi, le responsabilità, le risorse, i tempi di completamento. Il DPO monitora e verifica gli avanzamenti, valutando, al termine delle attività, l’efficacia di tali azioni.

**UTILIZZO DEI DATI AZIENDALI PER ACCESSO, RACCOLTA ED ELABORAZIONE DATI AZIENDALI PER FINALITÀ DI:**

* elaborazione tesi di laurea, ricerca, relazione, pubblicazione
* presentazione in Convegni, Seminari, Attività similari.

Si allega il modulo predisposto dall’Azienda, che dovrà essere utilizzato obbligatoriamente.