SISTEMA SANITARIO REGIONALE
ASL RIETI

REGIONE LAZIO

ASL DI RIETI

Procedura di gestione a norma privacy del Sistema Regionale “GIPSE”

Sommario

GIPSE 3
GIPSE E PRIVACY 3
ATTIVAZIONE DELLE UTENZE 4
GESTIONE E UTILIZZO DELLE UTENZE 6
MANUTENZIONE DEL SISTEMA 8
CONTROLLO SUL CORRETTO UTILIZZO DEL SISTEMA 8
ENTRATA IN VIGORE 9

GIPSE

Il sistema GIPSE attualmente in uso negli Ospedali della Asl di Rieti consente di gestire l'accoglienza del paziente, il *triage* e l'invio agli ambulatori, la cartella clinica di PS, la documentazione di legge, report e statistiche, export dati di interesse regionale ed aziendale.

L'interfaccia utente è strutturata in modo da lasciar visualizzare a ciascun utente del sistema GIPSE le informazioni che egli è abilitato ad inserire, le informazioni che può solo leggere, le informazioni obbligatorie ai fini della trasmissione all'Osservatorio Epidemiologico Regionale, le informazioni obbligatorie ai fini della chiusura della scheda PS oltre ad alcune altre informazioni il cui inserimento è facoltativo.

Il software permette, in tal senso, la creazione di diversi "profili-utente" abilitati ad operare con diversi livelli di visibilità dei dati e possibilità di intervento sugli stessi.

GIPSE E PRIVACY

È interesse primario della Asl di Rieti, in qualità di titolare del trattamento, garantire che ai dati personali trattati mediante lo strumento GIPSE possa accedere solo chi sia debitamente autorizzato per le finalità istituzionali per le quali lo stesso è stato attivato e che le informazioni, soprattutto quelle attinenti alla salute dei pazienti, siano adeguatamente protetti dai rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

In tal senso, appare opportuno formalizzare regole di accesso allo strumento compatibili con la vigente disciplina europea in materia protezione di dati personali dettata dal Regolamento EU/679/2016 (c.d. GDPR) e dalla normativa nazionale privacy (D. Lgs. n. 196/2003, come modificato dal D. Lgs. n. 101/2018 ("Codice Privacy") che protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali scongiurando, nel contempo, il verificarsi di violazioni di sicurezza che comportino, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Considerato che, ai sensi del primo comma dell'art. 5 del GDPR, i dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi

più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza») e che, ai sensi della medesima norma, "il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)", si ritiene necessario, mediante la presente procedura, regolamentare, a maggior tutela degli interessati e allo scopo di garantire adeguata protezione ai dati personali gestiti con GIPSE, le principali fasi di gestione e governo dello strumento attribuendo ad ognuno dei soggetti considerati i relativi ruoli e responsabilità.

Esula da quanto in questa sede considerato la puntuale individuazione della collocazione delle postazioni informatiche dalle quali è tecnicamente consentito l'accesso al GIPSE e i relativi presidi di sicurezza che, in ogni caso, dovranno essere del tutto assimilabili a quelli previsti per qualsivoglia sistema informatico della Asl di Rieti, in particolare per ciò che attiene alle caratteristiche di protezione e disponibilità dei dati, aggiornamento dei sistemi, idoneo posizionamento e adeguata gestione da parte delle persone autorizzate ad accedervi.

Ciò posto, nell'intero processo GIPSE si distinguono i seguenti momenti:

1) Attivazione delle utenze in uso al personale;
2) Utilizzo delle utenze;
3) Manutenzione del sistema;
4) Aggiornamento/dismissione delle utenze;
5) Controllo sul corretto utilizzo del sistema.

In riferimento a quanto precede, inoltre, vengono prese in considerazione le seguenti categoria di soggetti cui attribuire le corrispondenti responsabilità come meglio oltre specificate:

1) Il Direttore Sanitario del presidio ospedaliero;
2) Il direttore del Distretto 2
3) Il Direttore della UOC Pronto Soccorso e Medicina d'Urgenza;
4) I medici e il personale sanitario della struttura;
5) Gli Amministratori di sistema e la UOSD Sistema Informatico

ATTIVAZIONE DELLE UTENZE

Al fine di garantire il corretto utilizzo del sistema GIPSE è necessario fare in modo che allo strumento e ai dati con lo stesso trattati possa accedere solo chi sia dotato di adeguata autorizzazione.

In particolare, solo i soggetti cui lavorativamente competa la fruizione di GIPSE devono potervi accedere nel rispetto di un rigido criterio di segregazione dei ruoli.

A tale scopo, la Asl di Rieti ritiene di poter applicare al sistema stesso, quale criterio minimo di garanzia, i requisiti di sicurezza originariamente previsti dall'Allegato B) al D.Lgs. 196/2003 (c.d. Codice

privacy) laddove necessario opportunamente aggiornati in ragione del progresso tecnologico nel tempo intervenuto.

In tal senso, si prevede che il trattamento di dati personali mediante GIPSE venga consentito solo ai soggetti "autorizzati" ai sensi dell'art. 2-*quaterdecies* del Gdpr, come modificato dal D.Lgs 101/2018 dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione devono consistere in un codice per l'identificazione dell'autorizzato associato a una parola chiave riservata conosciuta solamente dal medesimo.

Ad ogni autorizzato possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione a patto che risultino tutte sempre riconducibili alla singola persona fisica.

Agli autorizzati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso.

La parola chiave in uso agli autorizzati deve risultare composta da almeno otto caratteri alfanumerici, non contenere riferimenti agevolmente riconducibili all'autorizzato medesimo ed essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi.

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

I profili di autorizzazione, per classi omogenee di autorizzati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Soggetto competente e responsabile per l'attivazione delle utenze GIPSE per quanto riguarda il personale sanitario afferente alla UOC MEDICINA E CHIRURGIA DI ACCETTAZIONE E D'URGENZA del presidio ospedaliero in cui è attivo GIPSE è il Direttore pro-tempore della medesima UOC cui spetta l'individuazione dei soggetti autorizzati e l'ambito di trattamento consentito a ciascuno.

Soggetto competente e responsabile per l'attivazione delle utenze GIPSE per quanto riguarda il personale sanitario afferente alle altre UOC del presidio ospedaliero la cui attività sia funzionalmente e necessariamente collegata alle prestazioni di medicina d'urgenza e pronto soccorso (consulenze, ecc.) è il Direttore Sanitario pro-tempore dell'Ospedale cui, previa richiesta scritta degli interessati veicolata tramite i rispettivi Direttori di UOC, spetta il compito di valutare la necessità dell'accesso – anche temporaneo – nonché l'ambito di trattamento consentito.

Soggetto competente e responsabile per l'attivazione delle utenze GIPSE per quanto riguarda il personale sanitario afferente al PPI (punto di primo intervento) presso la Casa della Salute di Magliano

Sabina in cui è attivo GIPSE è il Direttore pro-tempore del Distretto n. 2 cui spetta l'individuazione dei soggetti autorizzati e l'ambito di trattamento consentito a ciascuno.

Limitatamente al personale infermieristico, l'autorizzazione ad accedere al GIPSE viene concessa, secondo competenza, dai soggetti sopra indicati solo a seguito di richiesta formulata agli stessi dal Direttore pro-tempore del DIPARTIMENTO AZIENDALE PROFESSIONI SANITARIE che valuta la necessità dell'accesso – anche temporaneo – nonché l'ambito di trattamento consentito.

Spetta al Direttore Sanitario di presidio e/o al Direttore della UOC MEDICINA E CHIRURGIA DI ACCETTAZIONE E D'URGENZA e/o al Direttore pro-tempore del Distretto n. 2 richiedere per iscritto alla UOSD Sistema informatico della Asl di Rieti l'installazione ovvero la rimozione delle postazioni informatiche dalle quali si rende possibile l'accesso al GIPSE.

Spetta al Direttore Sanitario di presidio e/o, sentito il Direttore della UOC Medicina e Chirurgia di accettazione e d'Urgenza, dirimere eventuali contrasti in riferimento alla concessione, modifica o revoca, al singolo autorizzato o categoria omogenea di incaricati, delle credenziali di accesso a GIPSE.

Effettuata ogni necessaria valutazione, spetta al Direttore Sanitario di presidio e al Direttore della UOC MEDICINA E CHIRURGIA DI ACCETTAZIONE E D'URGENZA dello stesso presidio e/o dal Direttore pro-tempore del Distretto n. 2, secondo ragione, segnalare per iscritto, agli Amministratori di sistema allo scopo individuati all'interno della UOSD Sistema Informatico, la necessità di procedere alla creazione del profilo e all'attribuzione delle credenziali di accesso ai singoli richiedenti autorizzati.

Spetta, quindi, ai competenti Amministratori di sistema procedere, in ragione delle istruzioni in tal senso ricevute per iscritto, secondo ragione, dal Direttore Sanitario di presidio e dal Direttore della UOC MEDICINA E CHIRURGIA DI ACCETTAZIONE E D'URGENZA dello stesso presidio e/o dal Direttore pro-tempore del Distretto n. 2, alla creazione del profilo e all'attribuzione delle credenziali di accesso a GIPSE nei limiti e con le caratteristiche di interazione da questi predeterminate.

GESTIONE E UTILIZZO DELLE UTENZE

Ai soggetti cui viene riconosciuta l'attivazione di credenziali di accesso a GIPSE spetta l'obbligo di utilizzarle, in ossequio ad un criterio di stretta indispensabilità, nei limiti delle autorizzazioni ricevute e per il tempo strettamente necessario allo svolgimento della propria attività lavorativa.

La persona autorizzata, in particolare, all'esito dell'attività compiuta sulla cartella del singolo paziente ovvero allorché necessitata ad allontanarsi temporaneamente dalla postazione sulla quale opera, ha cura di disconnettersi dal sistema e/o di chiudere la cartella in questione onde non generare un rallentamento nell'accesso ai dati da parte degli altri sanitari e, soprattutto, della UOC Medicina e Chirurgia di accettazione e d'Urgenza.

La persona autorizzata è responsabile in proprio del carattere personale e riservato delle credenziali affidate e ha cura di custodirle in modo adeguato e non condividerle con terzi.

Spetta alle persone autorizzate non lasciare incustodito e accessibile, neppure temporaneamente, lo strumento elettronico mediante il quale accedono a GIPSE durante una sessione di trattamento.

Al Direttore Sanitario di presidio, anche su segnalazione scritta del Direttore della UOC Medicina e Chirurgia di accettazione e d'Urgenza, e/o al Direttore pro-tempore del Distretto n. 2 spetta il compito di richiamare gli assegnatari, ove necessario, ad un corretto uso delle credenziali e dei profili di accesso a GIPSE ivi compreso l'obbligo di disconnettersi dalla cartella del singolo paziente immediatamente dopo aver svolto l'attività per la quale avevano avuto accesso.

La ripetuta, ingiustificata, ovvero grave violazione delle regole di corretto accesso/gestione del GIPSE comportano, su decisione del Direttore Sanitario di presidio e/o del Direttore pro-tempore del Distretto n. 2, e/o Direttore della UOC Medicina e Chirurgia di accettazione e d'Urgenza, e la revoca temporanea o definitiva dei permessi di accesso.

Atteso che l'accesso a GIPSE degli operatori segue le regole di durata della password di dominio, la stessa scade ogni tre mesi. Credenziali non rinnovate alla scadenza non consentono l'accesso a GIPSE.

Le credenziali devono essere disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali ovvero in caso di cambiamento di ruolo che non preveda più il necessario accesso a GIPSE.

L'ambito di operatività delle credenziali deve essere aggiornato in ragione di eventuali cambiamenti di ruolo degli autorizzati con mantenimento dell'accesso a GIPSE.

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Spetta ed è responsabilità del Direttore Sanitario di presidio e/o al Direttore pro-tempore del Distretto n. 2, con la piena collaborazione degli Amministratori di sistema e della UOSD Sistema informatico della Asl di Rieti, il compito di procedere, nei tempi predetti, alle opportune verifiche per quanto riguarda gli incaricati afferenti alle UOC diverse da UOC MEDICINA E CHIRURGIA DI ACCETTAZIONE E D'URGENZA.

Spetta ed è responsabilità del Direttore della UOC MEDICINA E CHIRURGIA DI ACCETTAZIONE E D'URGENZA, con la piena collaborazione degli Amministratori di sistema e della UOSD Sistema informatico, procedere, nei tempi predetti, alle opportune verifiche per quanto riguarda gli incaricati afferenti alla UOC Medicina e Chirurgia di accettazione e d'Urgenza.

Limitatamente al personale infermieristico la verifica in questione viene effettuata sentito il Direttore pro-tempore del DIPARTIMENTO AZIENDALE PROFESSIONI SANITARIE.

MANUTENZIONE DEL SISTEMA

È di esclusiva competenza degli Amministratori di sistema allo scopo individuati all'interno della UOSD Sistema Informatico della Asl di Rieti qualsivoglia attività di manutenzione tecnica, anche su segnalazione dei singoli autorizzati, sul sistema GIPSE e in riferimento alle credenziali/profili di accesso.

Spetta, altresì, ed è di responsabilità della UOSD Sistema Informatico il corretto posizionamento e la sicurezza delle postazioni informatiche dalle quali si rende possibile l'accesso al GIPSE così come il collocamento e la rimozione, su richiesta scritta del Direttore Sanitario di presidio e/o del Direttore della UOC Medicina e Chirurgia di Accettazione e d'Urgenza e/o del Direttore pro-tempore del Distretto n. 2, delle postazioni stesse.

CONTROLLO SUL CORRETTO UTILIZZO DEL SISTEMA

Pur non costituendo in senso proprio un dossier sanitario elettronico, è indubbio che nel GIPSE confluiscono e vengono trattate una gran mole di dati personali attinenti alla salute dei pazienti che transitano per la Medicina d'Urgenza.

È parimenti indubbio che, per esclusive finalità lavorative, al sistema stesso possano legittimamente accedere un vasto numero di persone autorizzate con diversi profili di operatività.

Allo scopo di garantire ulteriormente la sicurezza delle informazioni trattate con GIPSE e i diritti e le libertà fondamentali degli interessati, questa Asl ritiene che costituisca buona prassi da perseguire l'applicazione anche a detto sistema di alcune delle cautele previste dall'Autorità Garante per la protezione dei dati personali nelle "Linee guida in materia di Dossier sanitario" del 4 giugno 2015.

In particolare, pur in assenza di disposizioni normative recanti obblighi in materia di tracciabilità delle operazioni con riguardo sia all'*an* sia al *quantum*, e comunque ferma restando la disciplina in materia di controllo a distanza dell'attività dei lavoratori, si ritiene utile applicare un sistema di controllo delle operazioni effettuate sul GIPSE che preveda la registrazione automatica in appositi file di *log* degli accessi e delle operazioni compiute sullo stesso programma.

In particolare, i file di *log* di GIPSE devono registrare per ogni operazione di accesso al sistema effettuata da un incaricato, almeno le seguenti informazioni: il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso; la data e l'ora di esecuzione; l'identificativo del paziente la cui scheda informatica è interessata dall'operazione di accesso da parte dell'incaricato e la tipologia dell'operazione compiuta sui dati.

In ragione della particolare delicatezza del trattamento dei dati personali effettuato mediante il GIPSE si ritiene necessario che siano tracciate anche le operazioni di semplice consultazione (*inquiry*).

Si prevede di implementare, all'atto di ogni accesso al sistema, un apposito avvertimento ***sul box "note operatore"*** che segnali all'incaricato l'esistenza del sistema di *log* come sopra definito e chiarisca che

si è ritenuto congruo stabilire che i *log* delle operazioni siano conservati per un periodo di 24 mesi dalla data di registrazione dell'operazione.

Gli incaricati sono informati del fatto che potrà essere svolta da parte della ASL di Rieti un'attività di controllo sui predetti log per il rilevamento di eventuali anomalie che possano configurare trattamenti illeciti.

I controlli, in particolare, comprendono verifiche sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento.

L'esito dell'attività di controllo è comunicato al Direttore Sanitario di presidio e/o al Direttore pro-tempore del Distretto n. 2 e/o al Direttore della UOC MEDICINA E CHIRURGIA DI ACCETTAZIONE E D'URGENZA i quali potranno disporre la revoca temporanea o definitiva dei permessi di accesso al GIPSE in caso di ripetuta, ingiustificata, ovvero grave violazione delle regole di corretto accesso/gestione del sistema e potrà essere messo a disposizione delle competenti Autorità, in caso di specifica richiesta ovvero di contenzioso.

ENTRATA IN VIGORE

La presente procedura entra in vigore all'atto della sua emanazione da parte della Direzione Generale.