

**Disciplinare tecnico in materia di misure di sicurezza  
prescritte per il trattamento dei dati nel sistema gestionale ELMAS**

Il titolare del trattamento, al fine di garantire un'adeguata tutela dei diritti e delle libertà degli interessati, nel contesto dell'operatività del sistema gestionale **ELMAS** per la gestione centralizzata e la digitalizzazione delle Dichiarazioni anticipate di trattamento (DAT) è tenuto alla rigorosa adozione delle misure di sicurezza individuate nel presente disciplinare tecnico.

La protezione dei dati deve essere assicurata tanto nella fase statica di archiviazione e conservazione, quanto in quella dinamica connessa ai processi di elaborazione ed eventuale comunicazione delle informazioni e per l'intero ciclo di vita dei dati, comprendente la fase di cancellazione o distruzione sicura delle informazioni non più soggette a trattamento.

Le misure di sicurezza definite nel presente disciplinare sono individuate, in conformità al dettato dell'art. 32 del GDPR, tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, così come del rischio di varia probabilità e gravità per i diritti delle persone fisiche.

Complessivamente, le misure tecniche prescritte sono finalizzate alla tutela dei diritti fondamentali, degli interessi e delle libertà dell'interessato, attraverso la salvaguardia dell'integrità, della disponibilità e della riservatezza dei dati oggetto di trattamento.

**1. FASE DI RACCOLTA E DI ACQUISIZIONE DEI DATI**

I dati personali comuni e categorie particolari dei dati personali relativi ai soggetti che intendono esprimere le proprie volontà in materia di trattamenti sanitari, nonché il consenso o il rifiuto rispetto ad accertamenti diagnostici o scelte terapeutiche e a singoli trattamenti sanitari - con l'eventuale indicazione di un fiduciario, che ne faccia le veci e la rappresenti nelle relazioni con il medico e con le strutture sanitarie - sono primariamente raccolti presso gli interessati da parte delle strutture sanitarie erogatrici pubbliche e private accreditate a contratto della Regione.

L'operatore autorizzato di ciascuna struttura sanitaria pubblica e privata della Regione abilitata al sistema gestionale ELMAS, previa verifica dell'identità del disponente, provvede alla produzione della copia scansata delle DAT e degli eventuali documenti allegati, apponendo su di essi gli estremi del protocollo.

Al fine di garantire la sicurezza del trattamento, prima della messa in produzione del sistema gestionale, è stata svolta un'analisi preliminare del rischio, le cui risultanze sono state formalmente documentate all'interno del verbale di "Privacy by Design e DPIA" redatto ai sensi dell'art. 35 del GDPR. Tale attività ha altresì comportato la necessità di individuare e formalizzare i ruoli e le responsabilità in capo ai soggetti coinvolti nel trattamento, nel rispetto del principio di *accountability*.

Il sistema gestionale è dotato dei necessari presidi di sicurezza, sia tecnici che organizzativi, atti a garantirne il corretto funzionamento nel rispetto dei principi previsti dalla normativa vigente in materia di protezione dei dati personali, nonché in coerenza con le *best practice* e gli standard internazionali di sicurezza delle informazioni, come illustrato nel presente disciplinare tecnico.

## **2. FASE DI ELABORAZIONE E GESTIONE DEI DATI**

Durante l'operatività del sistema gestionale vengono compiute operazioni di registrazione, modifica, consultazione ed estrazione, insistenti su dati personali comuni e su dati appartenenti a categorie particolari da parte del personale operante sul gestionale (personale delle strutture sanitarie erogatrici pubbliche e private accreditate a contratto della Regione), appositamente autorizzato al trattamento dei dati. Tali operazioni di trattamento sono funzionali allo svolgimento di tutte le attività necessarie all'erogazione del servizio di ricezione e trasmissione delle DAT alla Banca dati nazionale.

L'accesso al gestionale è riservato esclusivamente a soggetti preventivamente autorizzati e profilati, in funzione del ruolo e delle competenze operative loro attribuite, nel rispetto dei principi di minimizzazione, proporzionalità e necessità (cd. "*need to know*"), nonché di "*segregation of duties*" e del "*least privilege*".

È altresì previsto l'accertamento dell'identità personale degli utenti mediante meccanismi di autenticazione forte, secondo criteri che garantiscano sicurezza e certezza dell'identità. A titolo esemplificativo, l'autenticazione può avvenire tramite CNS rilasciata dal sistema TS, SPID di livello 2 rilasciato dagli Identity Provider accreditati, CIE emessa dal Ministero dell'Interno, firma remota o carta operatore SISS.

Il gestionale è configurato in modo da assicurare la tracciabilità completa delle operazioni effettuate dagli operatori autorizzati, attraverso sistemi di *log management* che consentono la registrazione automatica degli accessi e delle operazioni, con modalità idonee a garantirne l'integrità la disponibilità nel tempo.

A tutela della riservatezza e dell'integrità delle informazioni trattate, sono implementate tecniche di cifratura dei dati (cifratura sia in *transit* che *at rest*) e dei canali di comunicazione, mediante l'utilizzo di algoritmi conformi agli standard nazionali ed europei di sicurezza, nonché tecniche di *firewall*, sistemi di sicurezza perimetrale, *IDS/IPS*

e *hardening* dei server che consentono di monitorare e intercettare eventuali minacce alla sicurezza.

Sono, inoltre, previsti sistemi di backup dei dati, implementati secondo i migliori standard applicabili al contesto, al fine di garantire la continua disponibilità delle informazioni. Tali misure sono integrate da sistemi di *business continuity* e di *disaster recovery*, volti ad assicurare la resilienza del servizio anche in caso di eventi incidentali o interruzioni operativi.

Per il corretto funzionamento del gestionale è prevista la conduzione di attività di *Vulnerability Assessment* e *Penetration Test*, volte a verificare l'efficacia delle misure implementate.

### **3. PROCESSI DI COMUNICAZIONE**

Tutte le operazioni di comunicazione e scambio dei dati personali oggetto delle DAT avvengono esclusivamente mediante il gestionale ELMAS, che costituisce l'unico canale per la trasmissione dei dati alla Banca dati nazionale.

I flussi informativi transitano attraverso canali di comunicazione cifrati (crittografia *in transit* e *at rest*) e sistemi di autenticazione forte, in grado di garantire la riservatezza, l'integrità e la tracciabilità delle operazioni. Trovano applicazione le misure tecniche e organizzative di sicurezza descritte nei paragrafi precedenti.

### **4. CONSERVAZIONE DEI DATI**

I dati personali trattati nell'ambito del gestionale ELMAS sono conservati per il tempo strettamente necessario al perseguimento delle finalità di programmazione e monitoraggio dell'offerta sanitaria, nel rispetto dei principi di limitazione della conservazione e minimizzazione previsti dalla normativa in materia di protezione dei dati personali.

Durante la conservazione, i dati sono custoditi in ambienti sicuri e sottoposti a misure di protezione logica, fisica e organizzativa. In particolare, sono adottate a titolo esemplificativo e non esaustivo:

- la cifratura dei backup e dei supporti di memorizzazione, nonché la cifratura dei dati;
- la programmazione periodica dei backup e la verifica del corretto funzionamento attraverso test di *Restore* e prove di *Disaster Recovery*;
- l'applicazione di procedure di *business continuity*, volte a garantire la disponibilità dei dati anche in caso di guasti o interruzioni operative.

## **5. CESSAZIONE DEL TRATTAMENTO E CANCELLAZIONE DEI DATI**

Al termine del periodo di conservazione, i dati personali sono cancellati secondo procedure documentate, conformi alla normativa vigente in materia di protezione dei dati personali, mediante cancellazione fisica dei dati.

## **6. AGGIORNAMENTO DELLE MISURE DI SICUREZZA**

La sicurezza, ed in particolar modo la sicurezza informatica, deve essere necessariamente intesa come un processo soggetto a costante revisione ed aggiornamento. Le misure di sicurezza e le soluzioni tecniche considerate nel presente disciplinare sono, pertanto, sottoposte a periodiche attività di verifica e test al fine di accertarne l'efficacia. Tali misure possono, altresì, essere oggetto di periodico adeguamento, in ragione dello stato dell'arte disponibile, dei relativi costi di attuazione, nonché dell'eventuale definizione di ulteriori misure di garanzie prescritte ai sensi di legge.

Indipendentemente dalla fase di trattamento, sono inoltre previste misure di sicurezza organizzative e di governance, tra cui:

- l'erogazione di sessioni di formazione periodiche del personale in materia di sicurezza informatica e protezione dei dati personali;
- la valutazione preliminare dell'adeguatezza delle misure offerte dalle terze parti, che agiscono in qualità di responsabili del trattamento ex art. 28 del GDPR, nell'ambito del processo oggetto di analisi;
- l'esecuzione di verifiche di conformità in materia di protezione dei dati personali sulle terze parti, che agiscono in qualità di responsabili del trattamento, con conseguente aggiornamento delle misure di mitigazione;
- l'esecuzione di analisi periodiche del rischio e l'aggiornamento del verbale di "Privacy by Design e DPIA" ai sensi dell'art. 35 del GDPR;
- l'aggiornamento e l'esecuzione delle necessarie modifiche evolutive utili a consentire l'adattamento del sistema, anche in caso di nuovi requisiti imposti dalla normativa pro tempore vigente nell'ambito della protezione dei dati personali.