Ministero della Salute

Sistema informativo per il monitoraggio dell'assistenza primaria (SIAP)

Allegato 1: DISCIPLINARE TECNICO

Sommario

1. Introduzione

Il presente disciplinare tecnico descrive i contenuti informativi del *Sistema informativo per il monitoraggio delle prestazioni erogate nell'ambito dell'assistenza primarie* (SIAP), i soggetti coinvolti, le modalità tecniche per la trasmissione dei dati al Nuovo Sistema Informativo Sanitario (NSIS) e le garanzie di sicurezza e protezione per la trasmissione e l'utilizzo dei dati.
Ogni variazione significativa alle caratteristiche tecniche descritte nel presente disciplinare e, in generale, le novità più rilevanti, sono rese pubbliche sul sito internet del Ministero della salute (www.salute.gov.it), secondo le modalità previste dall'articolo 54 del Codice dell'amministrazione digitale.

2. Definizioni

Ai fini del presente disciplinare tecnico si intende per:

a. "crittografia", la tecnica per rendere inintelligibili informazioni a chi non dispone dell'apposita chiave di decifrazione e dell'algoritmo necessario;
b. "crittografia simmetrica", un tipo di crittografia in cui la stessa chiave viene utilizzata per crittografare e decrittografare il messaggio, ovvero una chiave nota sia al mittente che al destinatario;
c. "crittografia asimmetrica", un tipo di crittografia in cui ogni soggetto coinvolto nello scambio di informazioni dispone di una coppia di chiavi: una privata, da mantenere segreta; l'altra, da rendere pubblica. L'utilizzo combinato delle chiavi dei due soggetti permette di garantire l'identità del mittente, l'integrità delle informazioni e di renderle inintelligibili a terzi;
d. "sito Internet del Ministero", il sito istituzionale del Ministero della salute: **www.salute.gov.it**, accessibile dagli utenti per le funzioni informative relative alla trasmissione telematica dei dati;
e. "XML", il linguaggio di markup aperto e basato su testo che fornisce informazioni di tipo strutturale e semantico relative ai dati veri e propri. Acronimo di "eXtensible Markup Language" metalinguaggio creato e gestito dal World Wide Web Consortium (W3C);
f. "Centro Elaborazione Dati" o "CED", l'infrastruttura dedicata ai servizi di Hosting del complesso delle componenti tecnologiche del NSIS, dove i servizi di sicurezza fisica logica e organizzativa sono oggetto di specifiche procedure e processi;
g. "DGSISS", la Direzione Generale del Ministero della salute competente in materia di digitalizzazione, Sistema Informativo Sanitario e Statistica;
h. "Codice dell'Amministrazione Digitale" o "CAD", il decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni;
i. "cooperazione applicativa", l'interazione tra i sistemi informatici delle pubbliche amministrazioni effettuata nel rispetto delle regole tecniche di cui alle linee guida previste dall'art. 71 del CAD;
j. "tracciatura", registrazione delle operazioni compiute con identificazione dell'utente incaricato che accede ai dati;
k. "SPC", il Sistema Pubblico di Connettività di cui agli articoli 72 e seguenti del CAD;
l. "credenziali di autenticazione" i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
m. "utenti" o "utenti NSIS", il personale competente delle amministrazioni regionali e centrali.

3. I soggetti

Le Regioni e le Province autonome di Trento e di Bolzano trasmettono le informazioni e i dati relativi al SIAP attenendosi al presente disciplinare tecnico.
Le Regioni e le Province autonome di Trento e di Bolzano, ricevono i dati relativi al SIAP secondo modalità di trasmissione sicura definita a livello regionale/provinciale nei regolamenti di definizione del flusso e individuano, inoltre, un soggetto responsabile della corretta e tempestiva trasmissione dei dati al SIAP.

4. Descrizione del Sistema SIAP

4.1 Caratteristiche infrastrutturali

4.1.1 Aspetti generali

Date le peculiarità organizzative, le necessità di scambio di informazioni tra sistemi eterogenei e le caratteristiche dei dati trattati, il SIAP è basato su un'architettura standard del mondo Internet:

- utilizza lo standard XML per definire in modo unificato il formato e l'organizzazione dei dati scambiati nelle interazioni tra le applicazioni;
- attua forme di cooperazione applicativa tra sistemi;
- prevede una architettura di sicurezza specifica per la gestione dei dati personali trattati.

È costituito, a livello nazionale, da:

- un sistema che ospita il front-end web dell'applicazione (avente la funzione di web server);
- un sistema che ospita l'applicazione (avente la funzione di application server);
- un sistema dedicato alla memorizzazione dei dati (data server);
- un sistema dedicato alla autenticazione degli utenti e dei messaggi;
- un sistema dedicato a funzioni di Business Intelligence.

4.1.2 Misure idonee a garantire la continuità del servizio

A garanzia della corretta operatività del servizio, sono state attivate procedure idonee a definire tempi e modi per salvaguardare l'integrità e la disponibilità dei dati e consentire il ripristino del sistema in caso di eventi che lo rendano temporaneamente inutilizzabile. Tali misure sono periodicamente aggiornate sulla base delle evidenze che emergono dall'analisi dei rischi presentati dal trattamento che derivano in particolare dalla distruzione e dalla perdita dei dati.
In particolare, per quel che riguarda i dati custoditi presso il CED, sono previste:

- procedure per il salvataggio periodico dei dati (backup sia incrementale che storico);
- procedure che regolamentano la sostituzione, il riutilizzo e la rotazione dei supporti ad ogni ciclo di backup;
- procedure per il data recovery;
- procedure per la verifica dell'efficacia sia del backup che del possibile, successivo, ripristino;
- software aggiornato secondo la tempistica prevista dalle case produttrici ovvero, periodicamente, a seguito di interventi di manutenzione;
- basi di dati configurate per consentire un ripristino completo delle informazioni senza causarne la perdita di integrità e disponibilità;
- gruppi di continuità che, in caso di mancanza di alimentazione elettrica di rete, garantiscono la continuità operativa;
- soluzioni per la continuità operativa ed il disaster recovery.

La struttura organizzativa del CED e le procedure adottate consentono, in caso di necessità, di operare il ripristino dei dati in un arco di tempo inferiore ai sette giorni.

4.1.3 Misure idonee a garantire la protezione dei dati

4.1.3.1 Aspetti generali

Per garantire la protezione del patrimonio informativo del SIAP sono attivate misure di sicurezza fisica e logica idonee a salvaguardare l'integrità e la riservatezza delle informazioni. Tali misure sono periodicamente aggiornate sulla base delle evidenze che emergono dall'analisi dei rischi presentati dal trattamento che derivano in particolare dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati e prevedono:

- isolamento logico della rete;
- protezione dei dati e delle applicazioni da danneggiamenti provocati da virus informatici;
- autenticazione degli utenti;
- controllo dell'accesso alle applicazioni ed ai dati;
- integrità dei messaggi scambiati;
- cifratura dei dati.

Tutti i sistemi ospitati presso il CED sono collegati in rete locale e connessi alle infrastrutture comunicative attraverso servizi di firewall e proxy opportunamente configurati. Inoltre, la sicurezza degli stessi sistemi è incrementata mediante:

- strumenti IPS/IDS (Intrusion Prevention System/Intrusion Detection System) collocati nei punti di accesso alla rete al fine di consentire l'identificazione di attività ostili, ostacolando l'accesso da parte di soggetti non identificati e permettendo una reazione automatica alle intrusioni;
- un sistema di gestione degli accessi e di profilazione utenti, che prevede strumenti di autenticazione a più fattori;
- un sistema di registrazione delle operazioni di accesso degli utenti ai sistemi e delle operazioni di trattamento (sia tramite funzioni applicative o tramite accesso diretto), al fine di permettere l'individuazione di eventuali anomalie;
- un servizio SIEM (Security Information and Event Management) e un servizio SOAR (*Security orchestration, automation and response*), che realizzano le attività di logging, monitoraggio e correlazione degli eventi di sicurezza;
- un servizio di gestione Antivirus e Host IPS che centralizza la gestione delle componenti antivirus e HIPS (Host Intrusion Prevention System) al fine di prevenire intrusioni illecite e contrastare le minacce legate a software malevolo;
- utilizzo di uno strumento di controllo per l'accesso degli amministratori di sistema;
- utilizzo di uno strumento di controllo della gestione dei privilegi di accesso da parte degli amministratori delle basi di dati;
- utilizzo del canale HTTPS con protocollo TLS V1.2 o superiori;
- utilizzo di componenti di Trasparent Data Encryption (TDE) per proteggere i dati da utilizzi non autorizzati;
- funzioni di crittografia simmetrica e asimmetrica;
- separazione dei dati anagrafici dei soggetti censiti dai dati sensibili, con la predisposizione di distinti schemi di database.

4.1.3.2 Tracciatura delle operazioni effettuate sul sistema

Tutte le operazioni di accesso ai dati da parte degli utenti sono registrate e i dati vengono conservati in appositi file di log, al fine di evidenziare eventuali anomalie o utilizzi impropri, anche tramite specifici alert. Le informazioni registrate in tali file di log sono le seguenti:

- i dati identificativi del soggetto che ha effettuato l'accesso;
- la data e l'ora dell'accesso;
- l'operazione effettuata.

Inoltre, nel caso di accesso ai dati individuali, che può avvenire soltanto da parte degli amministratori di sistema, nei file di log è anche registrato il codice dell'assistito su cui è stato effettuato l'accesso.

Ai fini della verifica della liceità del trattamento dei dati:

- i log posseggono caratteristiche di integrità e inalterabilità;
- i log sono protetti con idonee misure contro ogni uso improprio;
- i log sono accessibili a personale opportunamente incaricato e autorizzato;
- i log sono conservati per 12 mesi e cancellati alla scadenza;
- i dati contenuti nei log sono trattati in forma anonima mediante aggregazione; possono essere trattati in forma non anonima unicamente laddove ciò risulti indispensabile ai fini della verifica della liceità del trattamento dei dati.

Nel caso di cooperazione applicativa:

- sono conservati i file di log degli invii delle informazioni al sistema;
- sono conservati i file di log delle ricevute del sistema;
- a seguito dell'avvenuta ricezione delle ricevute il contenuto delle comunicazioni effettuate è eliminato.

Tutte le operazioni di inserimento e aggiornamento dei dati prevedono la creazione di un messaggio in formato XML che viene firmato digitalmente dall'utente. Tutti i messaggi sono archiviati nel sistema per garantire la tracciabilità di tutte le modifiche dei dati.

4.2 Gestione dei supporti di memorizzazione

I supporti di memorizzazione, che includono nastri magnetici, dischi ottici e cartucce, possono essere fissi o rimovibili. Sui supporti di memorizzazione non vengono, comunque, conservate informazioni in chiaro; ciò malgrado, per ridurre al minimo il rischio di manomissione delle informazioni, viene identificato un ruolo di custode dei supporti di memorizzazione, al quale è attribuita la responsabilità della gestione dei supporti di memorizzazione rimovibili.
Per la gestione dei supporti di memorizzazione sono state adottate, in particolare, le seguenti misure:

- tutti i supporti sono etichettati a seconda della classificazione dei dati contenuti;
- viene tenuto un inventario dei supporti di memorizzazione;
- sono state definite ed adottate misure di protezione fisica dei supporti di memorizzazione;
- i supporti di memorizzazione non più utilizzati saranno distrutti e resi inutilizzabili, secondo procedure definite che prevedano la documentazione della distruzione.

4.3 Specifiche disposizioni per il trattamento dei dati identificativi dell'assistito

Come previsto dal Decreto del Ministro della salute 7 dicembre 2016, n. 262 (Regolamento recante procedure per l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, anche quando gestiti da diverse amministrazioni dello Stato), le Regioni e Province autonome effettuano, mediante procedure automatiche, prima dell'invio dei dati identificativi dell'assistito al Sistema NSIS:

1. la verifica di validità dei predetti codici identificativi;
2. la sostituzione dei predetti codici identificativi con i corrispettivi codici univoci prodotti da una funzione non invertibile e resistente alle collisioni.

La verifica di cui al punto 1, ammissibile solo nelle more dell'attivazione dell'Anagrafe Nazionale degli Assistiti ("ANA"), istituita ai sensi dell'articolo 62-ter del CAD, prevede uno scambio informativo con il servizio fornito dal sistema Tessera Sanitaria ("TS"), di cui alle disposizioni dell'articolo 50, del decreto legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326.
La funzione di cui al punto 2 è rappresentata da un algoritmo di hash che, applicato ad un codice identificativo (dato in input), produce un codice univoco (digest di output) dal quale non è possibile risalire al codice identificativo di origine. L'algoritmo di hash adottato è definito dalla DGSISS del Ministero della Salute ed è condiviso tra tutti i soggetti alimentanti, al fine di rendere il codice univoco non invertibile così ottenuto, a fronte del codice identificativo di input, unico sul territorio nazionale.
Il Codice univoco non invertibile (CUNI) così ottenuto rappresenta pertanto l'identificativo dell'assistito univoco sul territorio nazionale e dal quale non è possibile risalire all'identificativo di origine.
Il Ministero della salute, in fase di acquisizione dei dati, effettua la generazione ed assegnazione del codice univoco nazionale dell'assistito (CUNA) agli assistiti rappresentati dal CUNI, attraverso la diretta sostituzione del codice identificativo non invertibile ricevuto.
Il CUNA è generato mediante l'adozione di una funzione di Hash, rappresentata da un algoritmo definito dalla DGSISS, del codice identificativo non invertibile CUNI ricevuto.
Il CUNA è utilizzato come unico elemento identificativo dell'assistito nell'ambito di tutti i successivi trattamenti operati sul NSIS.

4.4 Sistema di autenticazione e autorizzazione degli utenti

4.4.1 Utenti del SIAP

Gli utenti del sistema sono individuati dal Ministero della salute e sono:

a) alle Aziende Sanitarie Locali, per i rispettivi ambiti territoriali di competenza, di consultare le informazioni rese disponibili dal SIAP in forma aggregata, a livello della propria azienda, su base mensile;

b) alle unità organizzative delle Regioni e Province autonome competenti, come individuate da provvedimenti regionali e provinciali, di consultare le informazioni rese disponibili dal SIAP in forma aggregata, a livello aziendale su base mensile e su propria competenza territoriale, anche al fine di effettuare analisi comparative sulle attività e prestazioni dell'assistenza sanitaria di base erogate, sulla base degli indicatori calcolati ai sensi dell'articolo 2, comma 4;

c) alle unità organizzative della Direzione generale competente in materia di programmazione sanitaria, della Direzione generale competente in materia di professioni sanitarie e della Direzione generale competente in materia di digitalizzazione e del sistema informativo e statistico sanitario nazionale del Ministero della salute, come individuate dal vigente regolamento di organizzazione, e all'AGENAS di consultare le informazioni rese disponibili dal SIAP in forma aggregata, a livello aziendale su base mensile.

Il Ministero della salute dispone di un sistema di autenticazione e autorizzazione, nonché di gestione delle identità digitali, attraverso il quale vengono definiti i profili di autorizzazione previsti per ogni sistema, definiti secondo le logiche del controllo degli accessi basato sui ruoli e declinati nello specifico in relazione al ruolo istituzionale, alle funzioni svolte e all'ambito territoriale delle azioni di competenza. Gli amministratori dell'applicazione, nominati dal Ministero della salute, gestiscono la designazione degli utenti e l'assegnazione dei privilegi di accesso.
Gli utenti accedono ai servizi del Ministero della salute attraverso dispositivi standard (Carta nazionale dei servizi, Carta di identità elettronica e SPID), definiti dalle vigenti normative, come strumenti per l'autenticazione telematica ai servizi erogati in rete dalle pubbliche amministrazioni ovvero, mediante strumenti di autenticazione a più fattori (MFA), in conformità all'art. 64 del CAD.
Il Ministero della salute adottano misure idonee ad attenuare il rischio connesso all'utilizzo fraudolento di identità digitali, suscettibili di comportare accessi abusivi e non autorizzati ai diversi sistemi e servizi, nonché idonee misure di conservazione delle password mediante funzioni crittografiche, in conformità alle Linee guida per la conservazione delle password, adottate con provvedimento del 7 dicembre 2023, doc. web. N. 9962283.
Per l'abilitazione all'accesso è previsto un processo come descritto nei successivi paragrafi.

4.4.2 Fase 1 - Abilitazione alla piattaforma

La prima fase prevede la registrazione da parte dell'utente, mediante l'inserimento delle generalità, del proprio indirizzo di posta elettronica e dei dettagli inerenti la struttura organizzativa di appartenenza, al fine di ricevere le credenziali di autenticazione. Successivamente, il sistema di registrazione invia una email contenente l'identificativo e la password che l'utente è obbligato a cambiare al primo accesso e, periodicamente, con cadenza definita sulla base delle evidenze che emergono dall'analisi dei rischi e anche a fronte di cambiamenti organizzativi o eventi anomali.
La parola chiave dovrà avere le seguenti caratteristiche:

- complessità (lunghezza e presenza di caratteri speciali) adeguata allo stato dell'arte tecnologico;
- non contenere riferimenti facilmente riconducibili all'incaricato.

Le credenziali di autorizzazione rispondono ai criteri definiti nel documento di password policy adottato dal Ministero della salute e, se non utilizzate per un periodo superiore a quello definito, sono disattivate.
Nelle more della definizione del quadro di garanzie e regole delle identità SPID ad uso professionale, è ammesso l'utilizzo di identità SPID ad uso personale escludendo l'uso di dati personali attinenti alla sfera privata del soggetto (es. e-mail e numero di cellulare personali, domicilio privato) forniti ai Service Provider.

4.4.3 Fase 2 - Abilitazione ai servizi

Nella seconda fase, l'utente può chiedere l'abilitazione ad un profilo del SIAP censito dal Ministero della salute e associato alla struttura organizzativa di appartenenza dell'utente.
L'amministratore dell'applicazione effettua un riscontro della presenza del nominativo nella lista di coloro che sono stati formalmente designati dal referente competente (ad es. della Regione o Provincia autonoma di appartenenza). Qualora questa verifica abbia esito negativo, la procedura di abilitazione si interrompe; nel caso in cui questa verifica abbia esito positivo, l'utente è abilitato all'utilizzo del sistema con appropriato profilo di accesso.
Per garantire l'effettiva necessità, da parte del singolo utente, di accedere alle informazioni per le quali ha ottenuto un profilo di accesso, le utenze vengono sottoposte a periodiche verifiche circa la sussistenza dei presupposti che hanno originato l'abilitazione degli utenti.

4.5 Modalità di trasmissione

4.5.1 Aspetti generali

La Regione o Provincia autonoma fornisce al SIAP le informazioni definite nelle successive sezioni, scegliendo fra le seguenti tre modalità alternative:

a) utilizzando le regole tecniche di cooperazione applicativa del Sistema Pubblico di Connettività (SPC) di cui all'art. 71 del CAD;
b) utilizzando i servizi applicativi web based che il Sistema mette a disposizione tramite il protocollo sicuro https e secondo le regole per l'autenticazione di cui al punto 4.3.1; il servizio applicativo permette l'upload delle informazioni;
c) ricorrendo alla autenticazione bilaterale fra sistemi basata su certificati digitali emessi da un'autorità di certificazione ufficiale.

I dati inviati al SIAP sono resi inintellegibili tramite crittografia asimmetrica utilizzando la chiave pubblica resa disponibile dal Ministero della salute.
A supporto degli utenti, il SIAP rende disponibile un servizio di assistenza raggiungibile mediante un unico numero telefonico da tutto il territorio nazionale; ogni ulteriore dettaglio è reperibile sul sito istituzionale del Ministero.
Le tempistiche di trasmissione ed i servizi di cooperazione applicativa sono pubblicati a cura del Ministero e sono reperibili sul sito istituzionale del Ministero.

4.5.2 Tempi di trasmissione

Il SIAP è alimentato con le informazioni inviate dalle Regioni e Province autonome secondo le tempistiche indicate dall'articolo 5 del decreto di istituzione del SIAP e devono essere raccolte al fine di consentire il monitoraggio delle prestazioni erogate nell'ambito delle attività e delle prestazioni erogate nell'ambito dell'assistenza sanitaria di base (cure primarie).

4.5.3 Sistema Pubblico di Connettività

Il Sistema Pubblico di Connettività (SPC) è definito e disciplinato all'art. 73 e seguenti del CAD.
Le trasmissioni telematiche devono avvenire nel rispetto delle regole tecniche del SPC, così come definito agli artt. 51 e 71 del CAD.

4.5.4 Garanzie per la sicurezza della trasmissione dei flussi informativi

Nel caso in cui la Regione o la Provincia autonoma disponga di un sistema informativo in grado di interagire secondo le logiche di cooperazione applicativa, l'erogazione e la fruizione del servizio richiedono come condizione preliminare che siano effettuate operazioni di identificazione univoca delle entità (sistemi, componenti software, utenti) che partecipano, in modo diretto e indiretto (attraverso sistemi intermedi) ed impersonando ruoli diversi, allo scambio di messaggi e all'erogazione e fruizione dei servizi.
In particolare, occorrerà fare riferimento alle regole tecniche individuate dall'art. 71 del CAD.
Nel caso in cui il sistema informativo della Regione o Provincia autonoma non corrisponda alle specifiche di cui sopra, l'utente che deve procedere all'inserimento delle informazioni può accedere al SIAP nell'ambito del NSIS ed inviare le informazioni attraverso una connessione sicura.

4.5.5 Standard tecnologici per la predisposizione dei dati

L'utente deve provvedere alla creazione e alla predisposizione di documenti conformi alle specifiche dell'Extensible Markup Language (XML) 1.0 (Fourth Edition) (raccomandazione W3C 29 settembre 2006).

Gli schemi standard dei documenti in formato XML contenenti le definizioni delle strutture dei dati dei messaggi da trasmettere, sono pubblicati, nella loro versione aggiornata, sul sito internet del Ministero della salute all'indirizzo **www.salute.gov.it**.

4.6 Servizi di analisi dati

I servizi applicativi consentono di accedere ad un'apposita funzionalità di reportistica che prevede diverse tipologie di utenti:

a) utenti del Ministero della salute;
b) utenti dell'Agenas;
c) utenti delle Regioni o Province autonome;
d) utenti delle Aziende Sanitarie Locali.

Il Ministero della salute ha realizzato strumenti online per il monitoraggio della completezza e qualità del caricamento dei dati SIAP e per l'analisi dei dati acquisiti in NSIS.
Tali strumenti sono rivolti ai valutatori ed a coloro che devono definire le politiche di programmazione a livello nazionale e regionale, nonché agli altri rilevanti stakeholders che operano nell'ambito delle attività e delle prestazioni erogate nell'ambito dell'assistenza sanitaria di base (cure primarie).

Gli strumenti disponibili nella piattaforma NSIS sono i seguenti:

i) reportistica dettagliata per il monitoraggio della completezza e qualità dei dati, in grado di evidenziare tempestivamente alle Regioni e P.A. eventuali errori e anomalie riscontrate nel flusso SIAP;
ii) sistema di indicatori tecnico-funzionali, per consentire ad ogni Regione e P.A. l'analisi dettagliata di informazioni rilevanti, anche attraverso l'integrazione tra flussi informativi diversi;
iii) dashboard di analisi dinamiche, a supporto dei processi di valutazione e programmazione sanitaria nell'ambito degli ospedali di comunità.

4.7 Informazioni

Il SIAP risponde all'esigenza di acquisire informazioni necessarie per monitorare le prestazioni erogate nell'ambito delle cure primarie, per monitorare l'adeguatezza delle cure e dell'assistenza agli standard qualitativi e quantitativi dei Livelli Essenziali di Assistenza (LEA), rilevando:

1. Caratteristiche anagrafiche, amministrative e sanitarie dell'assistito;
2. Motivazione e caratteristiche del contatto tra l'assistito e i servizi delle cure primarie del SSN;
3. Attività e prestazioni erogate dai servizi di cure primarie del SSN;
4. Caratteristiche organizzative delle strutture e dei presidi di erogazione delle cure primarie del SSN.

5. Ambito della rilevazione

Il SIAP intende raccogliere le informazioni riguardanti l'assistenza sanitaria erogata nell'ambito dell'assistenza sanitaria di base (cure primarie), rilevate dai professionisti sanitari e dalle strutture sanitarie censite nei modelli ministeriale STS11.

6. Le informazioni

6.1 Aspetti generali

Le regioni e le province autonome inviano i dati di cui all'articolo 3, esclusivamente in modalità elettronica in due tracciati distinti, di seguito indicati:

- DATASET 1 - che contiene le informazioni di carattere anagrafico dell'assistito;
- DATASET 2 - che contiene le informazioni relative alla prestazione e alla tipologia di contatto tra l'assistito e i servizi di cure primarie del SSN
- DATASET 3 - contiene le informazioni relative alle strutture e ai presidi di erogazione delle cure primarie

Le informazioni di dettaglio contenute nei 3 dataset sono indicate nelle tabelle di cui ai successivi paragrafi della sezione 6.

6.2 Dataset 1 – Anagrafica assistito

			Dataset 1 – Anagrafica Assistito	
Ambito informativo	**ID**	**Nome campo**	**Descrizione**	**Fonte**
DATI ANAGRAFICI	1	Codice Regione	Indica la Regione di assistenza dell'assistito	Regione
	2	Codice ASL	Indica il codice dell'azienda unità sanitaria locale che comprende il comune, o la frazione di comune, di assistenza dell'assistito	Regione
	3	Codice MMG/PLS	Indica il codice del MMG/PLS scelto dall'assistito	MMG/PLS
	4	ID_REC	Campo tecnico ottenuto dalla concatenazione dei campi chiave	Regione
	5	CUNI/CUNA	Codice Univoco Non Invertibile generato dalla Regione/ASL a partire dal CF dell'assistito	Regione/ASL
	6	Anno Nascita	Identifica l'anno di nascita dell'assistito	ARA*/ANA
	7	Genere	Indica il sesso dell'assistito	ARA*/ANA
	8	Cittadinanza	Identifica la cittadinanza dell'assistito	ARA*/ANA
	9	Comune di Residenza	Identifica il comune nella cui anagrafe (Anagrafe della Popolazione Residente) è iscritto l'assistito cui è stata erogata la prestazione	ARA*/ANA
	10	Comune di domicilio	Indica il comune di domicilio dell'assistito	ARA*/ANA

	11	Stato civile	Identifica lo stato civile dell'assistito nel periodo di riferimento della rilevazione	ARA*/ANA
DATI AMMINISTRATIVI	12	Codice di esenzione	Indica il codice di esenzione come da decreto del Ministero dell'economia di concerto con il Ministero della salute del 22 luglio 2005	ARA*/ANA
	13	Ambito e tipologia di esenzione	Indica l'ambito dell'esenzione	ARA*/ANA
	14	Data inizio validità esenzione	Indica la data di inizio validità dell'esenzione	ARA*/ANA
	15	Data fine validità esenzione	Indica la data di fine validità dell'esenzione	ARA*/ANA
	16	Data scelta	Indica la data di scelta del medico da parte dell'assistito.	ARA*/ANA
	17	Data revoca	Indica la data di revoca del medico da parte dell'assistito	ARA*/ANA
FATTORI DI RISCHIO	18	Fumo	Indica se assistito è fumatore	MMG/PLS
	19	Body Max Index (BMI)	Indica il valore del Body Max Index (BMI) dell'assistito	MMG/PLS
	20	Patologie croniche	Indica i problemi cronici dell'assistito (fino ad un massimo di 11) - cod. ICD-9-CM e successivi aggiornamenti	MMG/PLS

*ARA (Anagrafe Regionale assistiti) solo nelle more della piena attivazione di ANA (Anagrafe Nazionale Assistiti).

6.3 Dataset 2 – Contatto

Dataset 2 – Contatto				
Ambito informativo	**ID**	**Nome campo**	**Descrizione**	**Fonte**
DATI ANAGRAFICI	1	Codice Regione	Indica la Regione in cui è erogata la prestazione	Regione
	2	Codice ASL	Indica il codice dell'azienda unità sanitaria locale che comprende il comune, o la frazione di comune, in cui è erogata la prestazione	Regione
	3	Codice regionale medico	Indica il codice regionale del MMG/PLS	MMG/PLS
	4	ID_REC	Campo tecnico ottenuto dalla concatenazione dei campi chiave	Regione
	5	Data contatto	Indica la data in cui è avvenuto il contatto	MMG/PLS
	6	Progressivo del contatto	Indica il numero progressivo di contatti dell'assistito nella stessa giornata.	MMG/PLS

	7	Modalità contatto	Indica la tipologia del contatto	MMG/PLS
	8	Regime attività	Indica se il medico svolge la propria attività in "ciclo di scelta" o ad "attività oraria"	MMG/PLS
	9	Tipologia accesso	Indica se l'accesso è programmato (con prenotazione) oppure accesso diretto	MMG/PLS
PROBLEMA	10	Problema	Indica il problema di cui è affetto l'assistito (cod. ICD-9-CM e successivi aggiornamenti)	MMG/PLS
	11	Stato problema	Indica lo stato di evoluzione del problema	MMG/PLS
	12	Data apertura del problema	Indica la data in cui è stato aperto il problema	MMG/PLS
ATTIVITA E PRESTAZIONI	13	Tipologia di attività/prestazione	Indica la tipologia di attività/prestazione erogata	MMG/PLS
	14	Dettaglio prestazione	Indica il dettaglio rispetto alla tipologia indicata nel campo precedente	MMG/PLS
	15	Quantità erogata	Indica il numero di prestazioni o attività erogate riferite al dettaglio specificato	MMG/PLS

6.4 Dataset 3 – Organizzazione

Dataset 3 – Organizzazione				
Ambito informativo	**ID**	**Nome campo**	**Descrizione**	**Fonte**
STRUTTURA	1	Regione di erogazione	Indica la Regione a cui afferisce il medico che eroga la prestazione	MMG/PLS
	2	Azienda di erogazione	Indica l'Azienda Sanitaria Locale cui afferisce il medico che eroga la prestazione	MMG/PLS
	3	Codice regionale medico	Indica il codice identificativo a livello Regionale del medico	MMG/PLS
	4	Data contatto	Indica la data in cui è avvenuto il contatto.	MMG/PLS
	5	Progressivo del contatto	Indica il numero progressivo di contatti effettuati dallo stesso medico nella stessa giornata	MMG/PLS
	6	Codice Struttura	Indica la struttura in cui il medico sta erogando la prestazione, come codificata in STS.11	MMG/PLS
	7	Tipo Struttura	Indica il tipo di struttura	MMG/PLS
	8	AFT	Indica la AFT cui è associato il medico nel caso la struttura è Studio medico MMG, Studio medico PLS o Studio medico MMG/PLS	MMG/PLS
	9	UCCP	Indica la UCCP cui afferisce la AFT nel caso la struttura è Studio medico MMG, Studio medico PLS, Studio medico MMG/PLS o AFT	MMG/PLS

7. Tempistica trasmissioni

Le informazioni contenute nei suddetti Dataset, come stabilito nell'art. 5 del decreto di istituzione del SIAP, devono essere trasmesse su base settimanale, decorrente dalla data del contatto, entro la

settimana successiva a quella di riferimento delle stesse, a partire dal 1° gennaio 2027, considerando le settimane secondo lo standard ISO 8601.

Solo per l'anno 2026, le informazioni contenute nei suddetti Dataset sono trasmesse, con cadenza mensile, entro il mese successivo al mese di riferimento delle stesse.