REPUBBLICA ITALIANA

Regione Emilia-Romagna

BOLLETTINO UFFICIALE

DIREZIONE E REDAZIONE PRESSO LA PRESIDENZA DELLA REGIONE - VIALE ALDO MORO 52 - BOLOGNA

Parte prima - N. 38

Anno 50 **3 ottobre 2019** **N. 315**

REGIONE EMILIA-ROMAGNA

REGOLAMENTO REGIONALE 3 OTTOBRE 2019, N.5

MODALITÀ DI ATTUAZIONE E DI FUNZIONAMENTO DELL'ANAGRAFE REGIONALE DEGLI ASSISTITI (ARA) ISTITUITA CON L.R. 29 LUGLIO 2016, N. 13 E DISCIPLINA DELLE MODALITÀ DI SUBENTRO DELL'ARA ALLE ANAGRAFI DEGLI ASSISTITI DELLE AASSLL DELLA REGIONE EMILIA-ROMAGNA

IL PRESIDENTE DELLA GIUNTA REGIONALE EMANA

con decreto n.151 del 2 ottobre 2019

il seguente regolamento:

INDICE

Articolo 1

Definizioni

1. Ai fini del presente regolamento si intende per:

a) "AIRE" Residenti all'estero a cui è riconosciuto il diritto all'assistenza sanitaria limitata;

b) "ARA", Anagrafe Regionale degli Assistiti istituita dall'art. 14 della L.R. 29 luglio 2016, n. 13

c) "ASL di assistenza", l'Azienda Sanitaria Locale di iscrizione dell'assistito, che coincide con la ASL di residenza solo nel caso in cui il cittadino sia ivi residente;

d) "SSN", complesso di funzioni, strutture, servizi e attività che lo Stato garantisce a tutti i cittadini, senza alcuna distinzione, per il mantenimento e il recupero della salute fisica e psichica, nonché l'attuazione di sistemi di tutela della stessa, come vuole l'articolo 32 della Costituzione (Legge 23 dicembre 1978, n. 833);

e) "SSR", insieme delle strutture, delle funzioni e delle attività assistenziali rivolte ad assicurare, nell´ambito del Servizio sanitario nazionale e nel rispetto dei suoi principi fondamentali, la tutela della salute come diritto fondamentale della persona ed interesse della collettività ai sensi dell´art. 32 della Costituzione (art.1, Legge Regionale n. 29 del 23 dicembre 2004)".

f) "ASL di residenza", l'Azienda Sanitaria Locale che comprende il comune, o la frazione di comune, in cui risiede l'assistito;

g) "Assistito", soggetto iscritto volontariamente all'assistenza sanitaria nell'ambito del SSR;

h) "Assistibile", soggetto che ha diritto all'assistenza sanitaria nell'ambito del SSR;

i) "CAD", il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante "Codice dell'Amministrazione Digitale";

j) "Codice privacy", il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, recante "Codice in materia di protezione dei dati personali";

k) "ENI", cittadino dell'Unione Europea, specificatamente proveniente da Romania o Bulgaria, irregolarmente presente sul territorio e non iscritto al Servizio Sanitario Nazionale. Non è residente in un comune dell'ASL di assistenza.

l) "FSE", il Fascicolo Sanitario Elettronico, di cui all'articolo 12 del decreto legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni.

m) "MMG/PLS", i medici di medicina generale e pediatri di libera scelta;

n) "Piano di subentro", il Piano per il graduale subentro dell'ARA alle anagrafi e agli elenchi degli assistiti e assistibili tenuti dalle singole aziende sanitarie locali;

o) "PSU", straniero extracomunitario irregolare, temporaneamente presente sul territorio nazionale (es. migrante accolto nel progetto Mare Nostrum) e in possesso di permesso di soggiorno per motivi umanitari;

p) "Regolamento generale sulla protezione dei dati": Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE);

q) "STP", gli stranieri temporaneamente presenti ovvero i soggetti di cui all'articolo 35, commi 3 e 4, del decreto legislativo 25 luglio 1998, n. 286;

r) "Sistema TS": sistema informativo realizzato dal Ministero dell'Economia e delle Finanze in attuazione di quanto disposto dall'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326.

Articolo 2

Oggetto del regolamento

1. Il presente regolamento disciplina, ai sensi della legge regionale 29 luglio 2016, n. 13, articolo 14, le modalità di attuazione e di funzionamento dell'Anagrafe Regionale degli Assistiti (ARA) con particolare riferimento ai contenuti dell'ARA, alle modalità di raccolta e di trattamento dei dati anagrafici e sanitari, alle garanzie alle misure di sicurezza da adottare, nonché i criteri per l'interoperabilità dell'ARA con le altre banche dati di rilevanza nazionale e regionale.

Articolo 3

Funzionamento di ARA e modalità di subentro alle anagrafi e agli elenchi degli assistiti e assistibili tenuti dalle singole ASL

1. L'ARA assurge ad anagrafica di riferimento del Servizio Sanitario Regionale poiché consente l'identificazione univoca all'interno della Regione Emilia-Romagna degli assistiti e degli assistibili.

2. L'ARA subentra gradualmente alle anagrafi ed agli elenchi degli assistiti e assistibili tenuti dalle singole Aziende Sanitarie Locali (AASSLL), secondo un piano di avvio e messa in produzione concordato con le diverse Aziende coinvolte.

3. Nel subentro sono compresi tutti i dati relativi alle singole posizioni anagrafiche già presenti alla data del subentro nelle singole banche dati delle medicine di base aziendali.

4. A seguito del subentro, l'applicativo ARA diventa l'unica banca dati di riferimento della medicina di base, rendendo disponibili alle singole AASSLL e alla Regione Emilia-Romagna, i dati e gli strumenti necessari per lo svolgimento delle funzioni di rispettiva competenza.

Articolo 4

Modalità di funzionamento e informazioni trattate

1. L'ARA viene alimentata dalle AASSLL; la raccolta dei dati viene effettuata:

- acquisendo direttamente i dati anagrafici (es. nome, cognome, residenza….) dalle anagrafi comunali di competenza, dagli sportelli Unici Distrettuali o dagli sportelli CUP polifunzionali dell'ASL territorialmente competente;

- registrando le ulteriori informazioni (es. scelta/revoca del medico, fasce di reddito,….) anche di natura sanitaria (es. esenzioni per patologia) fornite dall'utente agli sportelli Unici Distrettuali, agli sportelli CUP polifunzionali dell'ASL territorialmente competente, ovvero mediante l'utilizzo dei servizi avanzati di sanità digitale, quali il FSE, per le informazioni direttamente gestibili dall'utente attraverso tali strumenti. Inoltre l'ARA riceve dal portale regionale e registra i riferimenti della DAT (Disposizione Anticipata di Trattamenti sanitari, come previsto dalla legge 219/2017), con particolare riferimento alle informazioni relative al luogo di deposito della DAT, agli estremi della DAT e alle informazioni sui fiduciari.

2. Nell'ARA sono contenute le informazioni di natura personale e sensibile riguardanti le seguenti categorie di soggetti:

a) assistibili dal SSR;

b) assistiti con iscrizione volontaria al SSR;

c) STP, ENI e PSU;

d) AIRE;

e) assistiti in carico a istituzioni estere (es. pensionati UE);

f) assistiti che per soggiorni brevi hanno diritto ad assistenza sanitaria limitata (es. Chernobyl).

3. Sono inoltre contenute in ARA le informazioni relative:

g) ai MMG/PLS del SSR (in termini di anagrafiche, incarichi, forme associative, dati ambulatori e massimali) per le funzionalità di scelta/revoca. L'ARA recepisce tali informazioni dall'applicativo regionale di gestione dei compensi dei medici MMG e PLS (denominato "Cedolino") che ne costituisce, ad oggi, la banca dati di riferimento;

h) ai codici delle esenzioni nazionali e regionali;

i) alle corrispondenze comuni-ASL in termini di dizionari di riferimento.

4. In ARA sono conservate, in una distinta sezione, le informazioni relative agli assistiti e agli assistibili non più iscritti, per un periodo di anni 30.

5. In ARA sono conservate le variazioni anagrafiche ed i dati relativi alle situazioni anagrafiche pregresse per un periodo di anni 30 dal decesso.

Articolo 5

Ruolo della Regione

1. La Regione assume il ruolo di Amministrazione owner dell'attività svolgendo funzioni di coordinamento e di controllo di coerenza dell'architettura informatica di ARA, delle modalità di realizzazione del progetto, della definizione delle strategie per l'evoluzione e la manutenzione tecnologica della stessa. Assicura, inoltre, la continuità operativa, livelli di performance adeguati e la sicurezza del sistema.

2. È istituita la Cabina di Regia composta da un rappresentante della Regione Emilia-Romagna e da un rappresentante

per ciascuna delle strutture sanitarie regionali.

3. La Cabina di Regia svolge funzioni di ricognizione dello stato di attuazione dell'ARA, di proposizione di soluzioni correttive e di miglioramento del sistema e di adeguamento ad eventuali modifiche normative incidenti sulle funzioni istituzionali delle strutture sanitarie.

4. La Cabina di Regia è composta da:

a. un referente per ciascuno dei servizi regionali coinvolti.

b. un referente ICT per ciascuna Area Vasta/Azienda Sanitaria.

c. due referenti del Dipartimento Cure Primarie per ciascuna Area Vasta/Azienda Sanitaria.

Articolo 6

Ruolo delle ASL regionali

1. Le ASL ai sensi dell'articolo 7 della legge 7 agosto 1982, n. 526 sono Titolari dei trattamenti dei dati relativi agli assistiti, agli assistibili ed ai medici convenzionati di propria competenza.

2. Le strutture sanitarie regionali fruiscono, ai sensi dell'art. 50 del D.Lgs. 82/2005, dei dati di cui all'art. 4 trattati da altre strutture sanitarie regionali quando l'utilizzazione di tali dati sia necessaria per lo svolgimento dei compiti istituzionali.

Articolo 7

Servizi resi disponibili dall' ARA

1. L'ARA rende disponibili inoltre le seguenti funzionalità di integrazione applicativa:

- Servizi di notifica verso i sistemi MPI (Master Patient Index) delle AASSLL, relativamente alle variazioni effettuate nell'ARA sugli assistiti, sugli assistibili e sui medici;

- Servizi di interrogazione delle posizioni contenute nell'ARA per le AASSLL, le Aziende Ospedaliere, gli IRCCS della Regione Emilia-Romagna e le Strutture Private e Accreditate. ARA, oltre a disporre di una modalità nativa, è integrata all'infrastruttura SOLE (servizi SAIARER e SAIA), al fine di mantenere la compatibilità con le integrazioni preesistenti. Le specifiche misure di sicurezza adottate sono allegate al presente regolamento – Allegato 2;

- Servizio di accesso all'applicazione integrato con i sistemi di autenticazione aziendale in dotazione alle AASSLL, alle Aziende Ospedaliere e IRCCS della Regione Emilia-Romagna.

- Servizi di interrogazione con l'anagrafe vaccinale.

Articolo 8

Clausola di invarianza finanziaria

1. Dall'attuazione del presente regolamento non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni interessate provvedono agli adempimenti previsti dal presente regolamento con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.

Articolo 9

Entrata in vigore

1. Il presente regolamento entra in vigore il giorno successivo alla sua pubblicazione nel Bollettino Ufficiale della Regione Emilia-Romagna Telematico.

Il presente regolamento sarà pubblicato nel Bollettino Ufficiale della Regione.

È fatto obbligo a chiunque spetti di osservarlo e farlo osservare come regolamento della Regione Emilia-Romagna.

Bologna, 3 ottobre 2019 STEFANO BONACCINI

MISURE DI SICUREZZA

Allegato al Regolamento **Modalità di attuazione e di funzionamento dell'Anagrafe Regionale degli Assistiti (ARA) istituita con L.R. 29 luglio 2016, n. 13 e disciplina delle modalità di subentro dell'ARA alle anagrafi degli assistiti delle AASSLL della Regione Emilia-Romagna**

1. Premessa

Il presente allegato descrive le caratteristiche della piattaforma e le misure adottate per garantire riservatezza, integrità e disponibilità dei dati trattati, nonché la sicurezza dell'accesso ai servizi, il tracciamento delle operazioni effettuate, in conformità agli articoli 64, comma 2 e 65, comma 1, lettera c), del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni (di seguito CAD).

2. Definizioni

Ai fini del presente allegato si intendono per:

a) "Certification Authority", è un ente di terza parte (trusted third party), pubblico o privato, abilitato a rilasciare un certificato digitale tramite procedura di certificazione che segue standard internazionali e conforme alla normativa europea e nazionale in materia;

b) "Credenziali di autenticazione", i dati e i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

c) "Profilo di autorizzazione", l'insieme delle informazioni, univocamente associate a una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

d) "Smart-card", ulteriore strumento di identificazione che, unitamente al PIN, è preposta all'autenticazione informatica;

i. "PIN", con questo acronimo si intende il Personal Identification Number, ovvero il codice associato all'identità digitale presente sul microchip della smart-card e consente al titolare il riconoscimento in rete e quindi la possibilità di accedere in modo sicuro e protetto ai servizi on-line messi a disposizione;

ii. "PUK", si tratta del PIN unlock key, ovvero il codice necessario per modificare il PIN assegnato o sbloccare la smart-card in caso di tripla digitazione errata del PIN.

e) "Backup", la replicazione delle informazioni al fine di prevenire la definitiva cancellazione o compromissione delle stesse a fronte di eventi accidentali o intenzionali che possano minacciarne l'integrità e la disponibilità;

f) "Disaster recovery", nell'ottica dell'art. 50 bis del CAD, l'insieme delle misure tecniche e organizzative adottate per assicurare, in siti alternativi a quelli primari di produzione, il funzionamento di tutti i servizi, a fronte di eventi che provochino, o possano provocare, l'indisponibilità prolungate.

3. Misure di sicurezza applicate ad ARA

Per le finalità di cui al paragrafo 1, l'ARA, realizzata presso un'infrastruttura di cui si dirà al paragrafo 3.1, è dotata di:

- un sistema di tracciamento e di conservazione dei dati di accesso alle componenti applicative e di sistema;

- sistemi di sicurezza per la protezione delle informazioni e dei servizi erogati dalla base dati;

- una Certification Authority;

- sistemi e servizi di backup per il salvataggio dei dati e delle applicazioni e di Disaster Recovery.

3.1 Infrastruttura fisica

I sistemi di produzione di ARA sono collocati presso il datacenter di Lepida s.c.p.a., a seguito dell'avvenuta fusione per incorporazione di CUP 2000 s.c.p.a. La sala è alimentata attraverso un impianto trifase distribuito internamente su linee elettriche ridondate. Un sistema d'alimentazione di riserva, realizzato con un gruppo elettrogeno alimentato a gasolio e possibilità di ricarica anche durante il funzionamento, garantisce l'autonomia del sistema anche in assenza di alimentazione dalla rete elettrica senza soluzione di continuità grazie alla commutazione automatica tra alimentazione ordinaria e alimentazione di riserva e ad UPS dedicati che alimentano la sala durante la commutazione. Il Datacenter di CUP2000 s.c.p.a. (ora Lepida s.c.p.a.) è stato progettato e costruito pensando alla ridondanza di tutte le parti critiche: sono presenti infatti internamente circuiti distinti di distribuzione elettrica, sistemi ridondati di climatizzazione, sistemi ridondati paralleli di trasporto dati per i servizi critici.

Contro i rischi di natura fisica, sia di tipo intrusivo che di tipo distruttivo, sono state previste delle misure idonee e adeguate alla probabilità e alla pericolosità del rischio. In dettaglio, la collocazione del Datacenter permette una vigilanza continua da parte del personale di centralino durante le ore di apertura degli uffici ed è chiuso a chiave e protetto da allarme volumetrico dedicato collegato a sistemi di continuità elettrica. Essendo completamente interno alla sede di CUP2000 Spa, nelle ore di chiusura degli uffici è protetto nei suoi accessi anche dal sistema di allarme della sede stessa. L'accesso al Datacenter, che è permesso solamente agli operatori in possesso del codice personale per il disinserimento dell'allarme e della chiave delle porte tagliafuoco, viene controllato e registrato elettronicamente.

Tutti i rack sono alimentati con cavi con guaina posati sotto al pavimento tecnico della sala e sono collegati al sistema di alimentazione ridondata. Il cablaggio dati, in categoria 6 e in fibra ottica, permette di avere connessioni fino a 10Gb ethernet all'interno del Datacenter fino alle connessioni con le reti esterne.

Il sistema di condizionamento del Datacenter è composto da unità di raffreddamento ridondate in logica N+1 che garantiscono all'interno della sala dati una temperatura di 21°C ± 3°C e l'umidità viene assicurata al 50% ± 10% grazie ad un sistema di umidificazione/deumidificazione automatico: in questo modo si ha la climatizzazione ottimale per il funzionamento delle macchine.

Il sistema di rilevazione e spegnimento incendi è composto da sensori ottici rivelatori di fumo e da sonde di temperatura, collocati sotto il pavimento flottante e a soffitto,

e da un sistema di spegnimento a scarica di gas Argon (gas inerte naturale ad impatto ambientale nullo ed alta capacità estinguente).

L'attivazione di qualsiasi sistema di sicurezza (allarme di intrusione, sistema antincendio, mancanza di alimentazione, avvio del generatore) viene segnalato automaticamente via telefono allo staff di gestione del Datacenter.

3.2 Registrazione degli utenti ed assegnazione degli strumenti di sicurezza

L'accesso al sistema ARA è possibile attraverso un'architettura distribuita basata su protocollo SAML 2.0 che garantisce l'identificazione degli utenti tramite i sistemi di autenticazione delle singole aziende sanitarie. La gestione delle credenziali utente (rilascio, rinnovo, policy di gestione, disattivazione) è pertanto demandata alle singole aziende sanitarie. Il sistema ARA non prevede un sistema di autenticazione locale.

L'accesso al sistema è inoltre possibile tramite Smartcard emesse da Certification Authority che emettono certificati di autenticazione CNS.

Una volta identificato l'utente tramite il sistema di autenticazione esterno o tramite smart card, l'accesso alle funzionalità applicative è regolato dalla profilazione utente. L'assegnazione del profilo autorizzativo al singolo utente viene effettuata direttamente sul sistema ARA.

Un utente può essere censito da un operatore deputato direttamente su ARA o attraverso il servizio di gestione delle utenze aziendali. In entrambi i casi l'amministratore del servizio di autenticazione deve assegnare direttamente su ARA, all'utenza appena creata, una o più opportune terne operative (azienda, ufficio, ruolo) in relazione a quella che dovrà essere la capacità operativa sul sistema ARA.

3.3 Protezione da attacchi informatici

Al fine di protezione dei sistemi operativi da attacchi informatici, eliminando le vulnerabilità, si utilizzano:

a) apposite procedure di profilazione al fine limitare l'operatività alle sole funzionalità necessarie per il corretto funzionamento dei servizi;

b) in fase di messa in esercizio, oltre che ad intervalli prefissati o in presenza di eventi significativi, processi di vulnerability assessment and mitigation nei software utilizzati e nelle applicazioni dei sistemi operativi;

c) piattaforma di sistemi firewall e sonde anti-intrusione.

3.4 Sistemi e servizi di backup e recovery dei dati soggetti al trattamento

I sistemi e servizi di backup per il salvataggio dei dati e delle applicazioni e di Disaster Recovery, vengono predisposti in conformità all'articolo 34, comma 1, lettera f), del decreto legislativo 30 giugno 2003, n. 196, e ai punti 18 e 23 dell'allegato disciplinare tecnico (Allegato B al decreto legislativo 30 giugno 2003, n. 196).

In particolare, al fine di assicurare la continuità delle operazioni indispensabili per il servizio e il tempestivo ritorno alla normale operatività, tutti i sistemi hardware e software coinvolti sono replicati presso in un secondo datacenter gestito da Lepida s.c.p.a. sito a Ravenna.

4. Accesso alla base dati

L'accesso ad ARA avviene in condizioni di pieno isolamento operativo e di esclusività, in conformità ai principi di esattezza, disponibilità, accessibilità, integrità e riservatezza dei dati, dei sistemi e delle infrastrutture, di cui all'articolo 51 del CAD.

I sistemi di sicurezza garantiscono che l'infrastruttura di produzione regionale sia logicamente distinta dalle altre infrastrutture e che l'accesso alla stessa avvenga in modo sicuro, controllato, e costantemente tracciato, esclusivamente da parte di personale autorizzato e con il tracciamento degli accessi.

ARA invia e riceve le comunicazioni in modalità sicura, su rete di comunicazione SPC ovvero, tramite Internet, mediante protocollo SSL per garantire la riservatezza dei dati su reti pubbliche.

4.1 Accesso da parte delle Aziende Sanitarie Locali

L'accesso ad ARA avviene tramite sito web e mediante web service.

4.1.1 Accesso tramite sito web dell'ARA

I requisiti di sicurezza prevedono il riconoscimento dell'operatore tramite il sistema di autenticazione dell'azienda sanitaria di appartenenza. L'identità dell'operatore viene comunicata ad ARA tramite protocollo SAML 2.0.

Il sistema ARA provvede ad associare all'utente un profilo di autorizzazione e di conseguenza ad abilitare le funzioni applicative relative.

Il sistema di tracciamento conserva le informazioni relative alla associazione utente dei dati modificati, inclusi i riferimenti temporali.

4.1.2 Accesso delle Aziende sanitarie locali e delle Regioni mediante web service

In questa seconda modalità di accesso, i requisiti di sicurezza prevedono:

- il riconoscimento dell'operatore tramite la userid e password utilizzata per accedere ai servizi dei sistemi informativi delle ASL/Regione, che garantiscono l'autenticazione dell'utente e la verifica dei diritti di accesso dello stesso alle varie funzionalità applicative;

- il certificato identificativo, riferito al server ospitante l'applicazione che utilizza il web service, memorizzato al suo interno, emesso dalla Certification Authority;

L'operatore accede autenticandosi tramite le credenziali ricevute ed utilizzate per accedere ai servizi dei sistemi informativi delle ASL/Regione.

Il sistema di tracciamento conserva le informazioni relative all'accesso degli utenti tramite web services.

Tutte le operazioni effettuate sono tracciate e conservate.

Le Aziende Sanitarie Locali, ovvero la Regione, garantiscono l'adeguamento delle applicazioni alle regole di sicurezza descritte.

LAVORI PREPARATORI

- Approvazione dello schema di regolamento regionale con deliberazione della Giunta regionale n.1110 del 1 luglio 2019;

- Espressione del parere di conformità con deliberazione dell'Assemblea legislativa n.220 del 17 settembre 2019;

- Approvato con deliberazione della Giunta regionale n.1595 nella seduta del 30 settembre 2019;

- Emanato dal Presidente della Giunta regionale con decreto n.151 del 2 ottobre 2019.

Documento firmato digitalmente da Caravita Lorella

Registrazione del Tribunale di Bologna n. 4308 del 18 dicembre 1973 – Proprietario: Giunta regionale nella persona del Presidente Stefano Bonaccini – Direttore responsabile: Giuseppe Pace – Responsabile Redazione: Lorella Caravita