REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

federfarma

Allegato sub b) alla Determinazione del Direttore Generale Dir. Gen. Sanità n. _____ del_____

ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI EX ART 28 REG. UE 679/2016

Tra

Regione Autonoma della Sardegna (di seguito per brevità "Regione"), Codice Fiscale 80002870923, rappresentata dal Direttore Generale della Sanità dell'Assessorato Igiene e Sanità e Assistenza Sociale, dott. Marcello Tidore,

e

Federfarma Sardegna - Unione Regionale dei Titolari di Farmacia - Regione Sardegna (di seguito per brevità "Farmacie"), Codice Fiscale 92016900927, con sede in Cagliari, via Biasi 25, rappresentata dal Presidente, dott. Giorgio Congiu, in qualità di rappresentante delle Farmacie che aderiscono alla Convezione per l'erogazione di servizi ICT del 07/03/2017, ai sensi dell'art. 3, lett. c) dello Statuto della Federfarma Sardegna;

il presente accordo sostituisce integralmente quello stipulato in precedenza e repertoriato al prot. n. 19017 rep. Convenzioni n. 11 del 30/07/2018.

INFORMAZIONI GENERALI

Titolare del Trattamento: Regione Autonoma della Sardegna – Presidente della Regione

Delegato del Titolare: Direttore Generale della Direzione della Sanità – Assessorato dell'igiene e sanità e dell'assistenza sociale
Indirizzo: via Roma, 223 - 09123 Cagliari
Telefono: 070 606 5361
Email: san.dgsan1@regione.sardegna.it
PEC: san.dgsan@pec.regione.sardegna.it

Responsabile della Protezione dei dati (DPO) per il sistema Regione Autonoma della Sardegna: Coordinatore Unità di progetto Responsabile della protezione dati per il sistema Regione Autonoma della Sardegna - Presidenza
Indirizzo: viale Trieste, 186 - 09123 Cagliari
Telefono: 070 606 5735
Email: rpd@regione.sardegna.it
PEC: rpd@pec.regione.sardegna.it

Responsabile del Trattamento: Farmacie aderenti alla Convenzione di cui all'Allegato 4.

DEFINIZIONI

"Normativa Nazionale Privacy": le norme italiane che disciplinano la protezione dei dati personali, ed in particolare il Decreto Legislativo 196/2003 e successive modifiche e integrazioni ed il D.Lgs. 10

agosto 2018 n. 101.

“Dato/i Personale/i”: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

“Interessato/i”: la/e persona/e fisica/che identificata/i o identificabile/i a cui si riferiscono i Dati Personali.

“Titolare”: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

“Responsabile”: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che tratta dati per conto del Titolare del trattamento dei dati personali.

“Responsabile della Protezione dei Dati”: la figura prevista dagli articoli da 37 a 39 del Regolamento UE 2016/679.

“Trattamento”: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

“Limitazione di trattamento”: il contrassegno dei dati personali conservati con l’obiettivo di limitarne il trattamento in futuro.

“Consenso dell’interessato”: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell’interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

“Violazione dei dati personali”: la violazione di sicurezza che comporta 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.

“Dati relativi alla salute”: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

“Pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

“Convenzione”: Convenzione per l’erogazione di servizi ICT presso le farmacie convenzionate tra la Regione Autonoma della Sardegna e Federfarma, tra l’Assessorato dell’Igiene e Sanità e dell’Assistenza Sociale della Regione Autonoma della Sardegna contratto Prot. .....del .....

PREMESSO CHE

- il Decreto del Presidente della Regione Sardegna, n. 10072/48 del 23/05/2018, recante ad oggetto "*Regolamento (UE) 2016/679 del Parlamento 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 (regolamento generale sulla protezione dei dati). Delega delle funzioni del Titolare del trattamento*", all'articolo 2, prevede che i Direttori Generali ed i responsabili apicali degli uffici possono esercitare le funzioni del Titolare del trattamento anche delegandole ai Direttori di Servizio pro tempore della medesima Direzione o Ufficio, secondo le relative competenze e responsabilità;
- la Regione Autonoma della Sardegna e Federfarma Sardegna hanno stipulato una convenzione disciplinante l'erogazione di servizi ICT presso le farmacie convenzionate (di seguito Convenzione);
- le attività oggetto della Convenzione comportano il trattamento di dati personali ai sensi del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito Regolamento o GDPR) nonché del D. Lgs. 196/2003 e ss.mm.ii. recante il Codice in materia di protezione dei dati personali;
- l'attuazione della Convenzione implica per le farmacie aderenti il trattamento di dati personali la cui titolarità è in capo alla Regione;
- il Titolare del trattamento di dati personali può preporre una persona fisica, una persona giuridica, una pubblica amministrazione e qualsiasi altro ente, associazione od organismo quale Responsabile al trattamento dei dati che sia nominato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo di sicurezza;
- nell'ambito dei servizi di cui alla presente Convenzione, Federfarma dichiara l'idoneità delle farmacie aderenti rispetto alle garanzie richieste dal Regolamento in particolare in termini di conoscenza specialistica, affidabilità e risorse per mettere in atto adeguate misure tecniche e organizzative a tutela della sicurezza del trattamento e dei diritti dell'interessato;
- è intenzione del Titolare consentire l'accesso sia al Responsabile che alle persone autorizzate al trattamento per i soli dati personali la cui conoscenza è necessaria per adempiere ai compiti loro attribuiti;
- il Responsabile deve procedere al trattamento secondo le istruzioni impartite dal Titolare per iscritto con il presente accordo e con eventuali accordi successivi;

TUTTO CIÒ PREMESSO

1. La Regione in qualità di Titolare dei dati cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali, nella persona del suo delegato, nomina le Farmacie aderenti alla Convenzione di cui all'Allegato 4 quali Responsabili del Trattamento ai sensi dell'art. 28

del Regolamento EU 2016/679 e della Normativa Nazionale Privacy, con l'incarico di effettuare le operazioni di trattamento sui dati personali relativi ai servizi oggetto della Convenzione.

2. Le Farmacie con la sottoscrizione del presente atto, accettano tutti i termini sotto indicati, confermano la diretta e approfondita conoscenza degli obblighi che si assumono in relazione al dettato normativo vigente e si impegnano a procedere al trattamento dei dati personali attenendosi alle istruzioni ricevute dal Titolare attraverso la presente nomina o a quelle ulteriori che saranno conferite nel corso delle attività prestate in suo favore.

3. Le Farmacie di cui all'Allegato 4, in qualità di Responsabili del trattamento si impegnano altresì ad attenersi "ALLE MISURE MINIME DI SICUREZZA" (Allegato 1) ed alle "ISTRUZIONI PER IL RESPONSABILE ALLE OPERAZIONI DI TRATTAMENTO DEI DATI PERSONALI E PARTICOLARI" (Allegato 2) che costituiscono parte integrante e inscindibile del presente accordo.

4. Le Farmacie prendono atto che qualsiasi mutamento dei requisiti di idoneità dichiarati, che possa sollevare fondati dubbi sul loro mantenimento, dovrà essere preventivamente segnalato al Titolare, che potrà esercitare in piena autonomia e libertà di valutazione il diritto di recesso, senza penali ed eccezioni di sorta.

ART. 1 PREMESSE E ALLEGATI

1.Le premesse e gli allegati, di seguito indicati, costituiscono parte integrante e sostanziale del presente Accordo e hanno valore di patto.

2. Il presente Accordo si compone dei seguenti allegati:

- Allegato 1 "MISURE DI SICUREZZA";
- Allegato 2 **"**ISTRUZIONI PER IL RESPONSABILE ALLE OPERAZIONI DI TRATTAMENTO DEI DATI PERSONALI E PARTICOLARI";
- Allegato 3 **"**DETTAGLIO DEI TRATTAMENTI";
- Allegato 4 "ELENCO DELLE FARMACIE".

ART. 2 OGGETTO

1. Oggetto del presente atto è la disciplina del trattamento dei dati personali che le Farmacie aderenti effettuano nell'ambito dei servizi di cui alla Convenzione.

2. Le Farmacie, Responsabili del trattamento, sono autorizzate a trattare, per conto del Titolare, i dati personali dei cittadini affinché gli stessi, presso la Farmacia, possano attivare/usufruire i seguenti servizi:

- attivazione della TS-CNS;
- attivazione della firma digitale;

- apertura del Fascicolo Sanitario Elettronico (FSE);
- consultazione del FSE;
- stampa e ritiro di documenti tramite il FSE (p.e. referti, certificati, etc.);
- scelta e revoca del medico;
- richiesta dell'esenzione per reddito dal pagamento del ticket;
- centro informazioni sui servizi online della Regione Sardegna.

ART. 3 NATURA E FINALITA' DEL TRATTAMENTO

La natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati sono specificati nell'Allegato 3 "DETTAGLIO DEI TRATTAMENTI" cui si rimanda.

ART. 4 DURATA E CESSAZIONE DEL TRATTAMENTO

1. Il trattamento ha una durata pari a quella di esecuzione della Convenzione e in ogni caso non superiore a quello necessario alla finalità per la quale i dati personali sono stati trattati. Tali dati devono essere conservati nei sistemi e nelle banche dati del Responsabile in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello in precedenza indicato ed a quanto previsto dall'art. 2220 del codice civile.

2. Al termine delle operazioni di trattamento affidate, nonché all'atto della cessazione per qualsiasi causa del trattamento da parte del Responsabile, lo stesso a discrezione del Titolare sarà tenuto a restituire al Titolare i dati personali oggetto del trattamento oppure, provvedere alla loro integrale distruzione salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge od altri fini (contabili, fiscali, ecc.).

In entrambi i casi il Responsabile provvederà a rilasciare al Titolare apposita dichiarazione per iscritto contenente l'attestazione che presso il Responsabile non esista alcuna copia dei dati personali e delle informazioni di titolarità del Titolare. Il Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertare la veridicità della dichiarazione. La presente nomina avrà efficacia fintanto che sia erogato il servizio, salvi gli specifici obblighi che per loro natura sono destinati a permanere. Qualora il rapporto tra le parti venisse meno o perdesse efficacia per qualsiasi motivo o il Servizio non fosse più erogato, anche il presente accordo verrà automaticamente meno senza bisogno di comunicazioni o revoche, ed il Responsabile non sarà più legittimato a trattare i dati del Titolare.

ART. 5 OBBLIGHI DEL TITOLARE

1. Il Titolare mette a disposizione del Responsabile quanto necessario per l'esecuzione della Convenzione ed in particolare:

- lettori smart card;
- accesso al portale;
- buste contenenti i codici PIN;
- informativa per il trattamento dei dati

2. Il Titolare si impegna a comunicare per iscritto al Responsabile qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati.

ART. 6 OBBLIGHI DEL RESPONSABILE

1. Il Responsabile tratterà i dati solo per la finalità o le finalità sopra specificate e per l'esecuzione delle prestazioni previste dalla Convenzione.

2. Il Responsabile dei dati personali si impegna a:

a) adempiere agli obblighi previsti dal GDPR e dalla Normativa Nazionale Privacy vigente, compreso l'obbligo di tenere un registro di tutte le categorie di attività di trattamento ai sensi dell'art. 30 del GDPR;

b) attenersi alle istruzioni del Garante per la protezione dei dati personali e, in particolare, alle misure di garanzia disposte dal Garante ai sensi dell'art. 2-septies del D.Lgs. 196/03;

c) trattare i Dati Personali solo se necessario per l'attivazione dei servizi ed osservare le istruzioni documentate del Titolare e come da questi comunicate per iscritto di volta in volta: qualora il Responsabile ritenga che un'istruzione di trattamento violi le leggi applicabili, informerà immediatamente al riguardo il Titolare e fornirà una motivazione adeguata;

d) fornire riscontro tempestivamente a tutte le richieste del Titolare in merito al trattamento dei Dati Personali;

e) vincolare il proprio personale che tratta i Dati Personali ad un adeguato obbligo di riservatezza, che rimane in vigore anche dopo il termine delle attività di trattamento; identificare e designare gli incaricati autorizzati ad effettuare operazioni di Trattamento sui Dati Personali, precisando l'ambito autorizzativo consentito ai sensi dell'art. 29 del GDPR e della Normativa Nazionale Privacy e provvedendo alla relativa formazione, fornendo le dovute istruzioni relativamente alle operazioni ed alle modalità di Trattamento dei Dati Personali, vigilando sulla puntuale applicazione delle istruzioni impartite e adottando misure disciplinari nei confronti di chi non rispetti tali istruzioni;

f) non divulgare o trasferire Dati Personali oggetto del presente accordo a terzi senza previa autorizzazione scritta del Titolare, eccetto laddove tale divulgazione o trasferimento siano richiesti per legge, nel qual caso il Responsabile informerà tempestivamente il Titolare per iscritto prima di adempiere a tali richieste di divulgazione; il Responsabile dovrà rispettare tutte le indicazioni del

Titolare in relazione a tale divulgazione o trasferimento;

g) non trasferire i Dati Personali in un paese al di fuori dello Spazio Economico Europeo che non preveda un livello di protezione dei dati equivalente a quello dell'Unione Europea come riconosciuto da una decisione della Commissione Europea, senza previa autorizzazione scritta del Titolare; in ogni caso, il Responsabile collaborerà con il Titolare per assicurarsi che siano in vigore adeguate salvaguardie legali o contrattuali per tali trasferimenti internazionali in conformità alla legislazione applicabile;

h) fornire un'assistenza al Titolare nel rispettare i suoi obblighi di trasparenza nei confronti degli interessati;

i) informare tempestivamente il Titolare di qualsiasi comunicazione ricevuta dagli interessati in relazione all'esercizio dei loro diritti sui propri Dati Personali e rispettare le istruzioni del Titolare nel fornire riscontro a tali comunicazioni;

j) informare gli interessati sul trattamento dei propri Dati Personali in conformità alle leggi applicabili e alle istruzioni del Titolare ogni volta che il Responsabile del trattamento raccoglie Dati Personali direttamente dagli interessati per conto del Titolare;

k) adottare misure tecniche e organizzative adeguate previste dal GDPR e dalla Normativa Nazionale Privacy, cosi come ogni altra previsione derivante dall'Autorità di Controllo, ovvero dal Comitato Europeo per la protezione dei dati e comunque in conformità con l'art. 5, lettera f, ed all'art. 32 del GDPR per proteggere i Dati Personali da distruzione accidentale o illecita o perdita o danno accidentale, alterazione, divulgazione o accesso non autorizzati e da tutte le altre forme di trattamento non autorizzate o illegali o richieste dalle leggi applicabili;

l) ad adottare e mantenere appropriate misure di sicurezza di cui all'art. 32 del GDPR, sia tecniche che organizzative, per proteggere i Dati Personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati, ed in particolare, laddove il trattamento comporta trasmissioni di dati su una rete, da qualsiasi altra forma illecita di trattamento.
A tal fine il Responsabile del trattamento si impegna a rispettare i Requisiti Minimi di Sicurezza stabiliti dal Titolare del Trattamento di cui al successivo Allegato 1 e i provvedimenti in materia del Garante per la protezione dei dati personali, ivi incluso il provvedimento del 27 novembre 2008 in materia di amministratori di sistema, fatti salvi gli adeguamenti che potranno essere necessari a seguito dell'applicazione del Regolamento e di suoi eventuali provvedimenti attuativi. Tra le misure tecniche ed organizzative che garantiscono un livello di sicurezza adattato al rischio, ivi compresi, sono comprese fra le altre:

a) la pseudonimizzazione e la cifratura dei dati personali

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
L'adesione a un codice di condotta o una certificazione può essere utilizzata dal Responsabile,

come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 dell'art. 32 del GDPR;

m) fornire al Titolare la documentazione tecnica relativa alle procedure, eventualmente poste in essere, per testare e valutare l'efficacia delle misure tecniche e organizzative per la sicurezza del trattamento;

n) rispettare la vigente disciplina sugli amministratori di sistema (in origine contemplata dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008) e conservare gli estremi identificativi delle persone fisiche preposte alla mansione di amministratore di sistema e il registro delle attività dagli stessi poste in essere;

o) verificare periodicamente e, comunque, almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati e/o responsabili del trattamento e/o amministratori di sistema nominati;

p) astenersi dal compiere qualsiasi trattamento di dati personali che non sia stato definito in Convenzione e/o che comunque abbia finalità diverse da quelle definite e consentite;

q) garantire l'affidabilità di qualsiasi dipendente che accede ai Dati Personali di cui è titolare la Regione Sardegna ed assicurare, inoltre, che gli stessi abbiano ricevuto adeguata formazione con riferimento alla protezione e gestione dei Dati Personali, e che siano vincolati al rispetto di obblighi di riservatezza non meno onerosi di quelli previsti nel presente Accordo relativamente al Trattamento dei Dati Personali.

In ogni caso il Responsabile del trattamento dei dati sarà direttamente ritenuto responsabile per qualsiasi divulgazione di Dati Personali che dovesse realizzarsi ad opera di tali soggetti;

r) tenere conto, utilizzando i materiali, i prodotti, le applicazioni o i servizi, dei principi di protezione dei dati a partire da quando questi vengono progettati e della protezione dei dati di default;

s) informare il Titolare per iscritto secondo la procedura di data breach di cui alla DGR 51/3 del 16/10/2018, di qualsiasi distruzione accidentale o illecita o perdita o danno accidentale, alterazione, divulgazione o accesso ai Dati Personali non autorizzati, fornendo tutti i dettagli completi della violazione subita ed attivandosi per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare ed attuando tempestivamente tutte le azioni correttive approvate e/o richieste dal Titolare. In particolare, il Responsabile dovrà fornire una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Titolare e sugli Interessati coinvolti e le misure adottate per mitigare i rischi; il Responsabile dovrà assistere il Titolare nell'obbligo, in conformità con le leggi applicabili, di notificare la violazione alle autorità di controllo competenti e agli Interessati, nella misura in cui il Responsabile del trattamento disponga di informazioni rilevanti per il Titolare al fine di adempiere ai propri obblighi di notifica;

t) informare tempestivamente il Titolare di eventuali ispezioni e misure adottate dalle Autorità di controllo, nella misura in cui incidano sulle operazioni di trattamento ai sensi del presente atto. Ciò vale anche, nella misura consentita dalla legge applicabile, laddove il Responsabile sia oggetto di indagine o sia parte di un'indagine condotta dall'autorità pubblica relativa ai Dati Personali trattati ai sensi del presente accordo. Il Responsabile dovrà conformarsi a tutte le indicazioni del Titolare in merito a qualsiasi divulgazione o trasferimento di Dati Personali alle autorità competenti;

u) assistere il Titolare, qualora sia fatta richiesta specifica in tal senso, nell'ambito delle procedure dinnanzi all'Autorità di controllo o all'Autorità Giudiziaria per le attività di sua competenza;

v) applicare senza indebito ritardo adeguate misure di sicurezza e di mitigazione, in accordo con il Titolare, per limitare i potenziali effetti negativi di una violazione della sicurezza;

w) assistere il Titolare nell'effettuare valutazioni di impatto sulla protezione dei dati e preparare le consultazioni con le autorità di controllo, laddove il Responsabile detenga informazioni rilevanti affinché il Titolare rispetti gli obblighi previsti dalle leggi applicabili;

x) il Responsabile del trattamento dei dati accetta che il Titolare o un revisore esterno incaricato dal Titolare possa, con ragionevole preavviso, ispezionare e verificare il trattamento dei Dati Personali per confermare l'adempimento degli obblighi stabiliti nel presente atto e nelle leggi applicabili da parte del Responsabile. La verifica può, tra l'altro, comportare richieste di informazioni o un'ispezione dei locali del Responsabile da parte del Titolare o del revisore esterno incaricato;

y) il Responsabile fornirà al Titolare o al revisore esterno incaricato tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla presente nomina e tutto il materiale necessario affinché il Titolare possa condurre tali ispezione o audit;

z) esporre all'interno della farmacia e ben visibile al pubblico le informative.

ART. 7 MANLEVA

Il Responsabile si obbliga a manlevare e a tenere indenne il Titolare da qualsiasi danno, pregiudizio, costo, spesa per comportamenti commissivi/omissivi connessi al proprio ruolo di Responsabile nonché dei propri incaricati del trattamento e/o responsabili interni del trattamento e/o amministratori di sistema e/o eventuali sub-responsabili.

ART. 8 COMUNICAZIONI TRA LE PARTI

Le comunicazioni tra le parti, ai fini del presente incarico, dovranno essere indirizzate:

- per il Titolare del trattamento: Regione Autonoma della Sardegna – Direzione Generale della Sanità via Roma n. 223 – Cagliari,

  Tel. 070 606 5361,

  PEC: san.dgsan@pec.regione.sardegna.it.

- per il Responsabile del trattamento: Federfarma Sardegna - Unione Regionale dei Titolari di Farmacia - Regione Sardegna, via Biasi 25- Cagliari,

  Tel. 070099701 –

  PEC ur.sardegna@pec.federfarma.it

  email: segreteria@federfarmacagliari.it.

ART. 9 DISPOSIZIONI FINALI

1. La Nomina non prevede alcun compenso aggiuntivo in favore del Responsabile.

2. Per quanto non espressamente ivi previsto, si rinvia alle disposizioni generali vigenti in materia di protezione di dati personali.

3. Con il presente accordo si intende espressamente revocare e sostituire ogni altro accordo tra le parti inerente il trattamento di dati personali.

4. Il servizio di apertura del FSE e le operazioni connesse rimarranno operative nelle more della completa definizione, attuazione e completamento delle attività di attivazione massiva per tutta la popolazione conseguenti all'abrogazione del consenso all'alimentazione ai sensi dell'art. 11 del Decreto Legge 19 maggio 2020, n. 34 (c.d. Decreto Rilancio), fermo restando che dovrà rimanere sempre operativo il servizio di gestione del consenso alla consultazione del FSE.

Il Titolare Il Responsabile

Allegato 1

MISURE DI SICUREZZA

PREMESSA

Scopo

Il presente documento descrive le misure di sicurezza che devono essere adottate ai fini della protezione delle informazioni e dei dati personali, al fine di garantire la sicurezza del trattamento ai sensi dell'art. 32 del REG UE 2016/679.

Il rispetto di queste misure di sicurezza non garantisce che sia stato fornito un adeguato livello di protezione, in quanto una valutazione globale di sicurezza dovrà essere effettuata dal Responsabile secondo il contesto in cui opera, il tipo di dati e il tipo di trattamento da dover eseguire.

Le informazioni tecniche in materia di sicurezza e le minacce alla sicurezza sono in continua evoluzione. La sicurezza deve essere continuamente oggetto di valutazione alla luce delle circostanze specifiche per determinare il livello di protezione appropriato.

Tali requisiti devono essere rispettati da tutte le Farmacie che Trattano Dati Personali per conto dell'Assessorato dell'Igiene e Sanità e dell'Assistenza Sociale della Regione Autonoma della Sardegna, Titolare del trattamento che sono definite, nel presente allegato, "Responsabili del trattamento".

Resta inteso che i presenti requisiti devo essere integrati con le ulteriori garanzie in materia di sicurezza concordate con l'Assessorato dell'Igiene e Sanità e dell'Assistenza Sociale con ogni ulteriore requisito di sicurezza, individuato nel corso di qualsiasi di valutazione della sicurezza effettuata, sia prima che dopo la stipula del contratto.

Misure di Sicurezza Standard

Misure organizzative

Responsabile della Protezione dei dati

1. Nei casi previsti dall'art. 37 del REG UE 679/2016, è designato un Responsabile della Protezione dei dati a cui è affidata la verifica della *compliance* con i presenti requisiti minimi di sicurezza. Detto soggetto deve essere adeguatamente formato, esperto nella gestione della protezione delle informazioni e dei dati e dotato di risorse adeguate per garantire efficacemente la *compliance*.

Piano sulla Sicurezza

2. Le misure adottate per conformarsi ai presenti requisiti minimi di sicurezza sono oggetto di un piano di sicurezza, che deve essere mantenuto fino ad una determinata data e rivisto ogni volta che vengono apportate modifiche rilevanti al Sistema informativo o alla sua organizzazione. Il documento di sicurezza deve registrare i cambiamenti significativi relativi alle misure di sicurezza o alle attività di Trattamento.

3. Il Piano di Sicurezza deve comprendere almeno:

a. Meccanismi di protezione dei dati per garantire l'integrità e la riservatezza dei dati; la classificazione dei dati stessi;
b. un piano di Disaster Recovery che precisi: le misure per ridurre al minimo le interruzioni del normale funzionamento del sistema; le misure per limitare la portata di eventuali danni e disastri; le misure per consentire una transizione graduale dei Dati Personali da un sistema ad un altro; se necessario, la previsione di mezzi alternativi per garantire i funzionamento di un sistema;
c. un Piano di emergenza che consenta di affrontare possibili pericoli che possono incombere sui dati personali gestito dal Responsabile per conto del Titolare del Trattamento;
d. La sicurezza dei computer e dei sistemi di telecomunicazione, incluse le procedure per la gestione delle copie di back-up, le procedure di contrasto ai virus, le procedure per la gestione di segnali/codici, la sicurezza per implementazione del software, la sicurezza dei database, la sicurezza dei sistemi di collegamento a Internet, i controlli su eventuali tentativi di aggiramento di detti sistemi, i meccanismi per tenere conto dei tentativi di violazione della sicurezza del sistema o di ottenere un accesso non autorizzato.

Funzioni e obblighi del personale

4. Solo i dipendenti che siano dotati di adeguata onestà, integrità e discrezione devono essere i Soggetti Autorizzati e avere l'accesso ai locali dove si trovano i Sistemi Informativi o i Supporti contenenti Dati Personali. Il Personale deve essere vincolato da un obbligo di riservatezza nei confronti di qualsiasi accesso ai Dati Personali.

5. Devono essere adottate le misure necessarie per formare il personale e renderlo competente a rispettare i presenti requisiti minimi di sicurezza, ogni pertinente disciplina o policy applicabile e/o rilevante per le attività loro affidate, gli obblighi in materia di trattamento dei Dati Personali e le conseguenze di qualsiasi violazione di questi obblighi.

6. Le funzioni e gli obblighi del personale che ha accesso ai Dati Personali e ai Sistemi Informativi devono essere chiaramente definiti e documentati.

7. I Soggetti Autorizzati sono istruiti affinché le apparecchiature elettroniche non siano lasciate incustodite e rese accessibili durante le sessioni di Trattamento.

8. L'accesso fisico alle aree dove vengono conservati i Dati Personali deve essere limitato ai Soggetti Autorizzati.

Misure Tecniche

Autorizzazione

9. Possono accedere ai Sistemi Informativi o ad effettuare un Trattamento dei Dati Personali esclusivamente i dipendenti sono autorizzati al trattamento.

10. Deve essere previsto un sistema di autorizzazione qualora vengano utilizzati profili di autorizzazione differenziati per diversi scopi di trattamento.

Identificazione

11. Ogni Soggetto Autorizzato deve essere associato ad un codice di identificazione unico e personale ("User ID").

12. Un ID Utente non può essere assegnato ad un'altra persona, neanche in un momento successivo.

13. Deve tenersi un elenco aggiornato degli Utenti Autorizzati e del profilo di autorizzazione assegnato a ciascuno; le procedure di identificazione e di autenticazione devono essere previste per tutti gli accessi ai Sistemi Informativi o per il compimento di qualsiasi Trattamento dei Dati Personali.

Autenticazione

14. I soggetti Autorizzati sono ammessi al Trattamento di Dati Personali se sono dotati di credenziali di autenticazione che consentano di completare con successo una procedura di autenticazione relativa a una specifica operazione di Trattamento o a un insieme di operazioni di Trattamento.

15. L'autenticazione deve avvenire tramite SPID Livello 2 o CNS.

16. Le istruzioni fornite ai soggetti Autorizzati devono prevedere l'obbligo, come condizione per l'accesso ai Sistemi Informativi, di prendere le precauzioni necessarie a garantire che la componente segreta delle credenziali di autenticazione sia mantenuta riservata e che i dispositivi utilizzati e tenuti esclusivamente dai soggetti Autorizzati siano tenuti con la dovuta cura.

17. Le credenziali di autenticazione devono essere disattivate se non sono state utilizzate per almeno sei mesi, ad eccezione di quelle che sono state autorizzate esclusivamente per finalità di gestione e supporto tecnico.

18. Le credenziali di autenticazione devono essere anche disattivate se il soggetto Autorizzato è de- qualificato o non più autorizzato all'accesso ai Sistemi Informativi o al Trattamento dei Dati Personali.

19. Laddove i dati e le apparecchiature elettroniche siano accessibili solo utilizzando le componenti riservate delle credenziali di autenticazione, sono fornite indicazioni appropriate, in anticipo e per iscritto, per specificare chiaramente le procedure con cui il Responsabile del trattamento può garantire l’accesso ai dati o alle apparecchiature elettroniche nell’eventualità in cui l’incaricato del trattamento sia assente o non disponibile per un lungo tempo e l’accesso a tali apparecchiature e/o ai dati sia indispensabile per svolgere determinate attività, senza ritardo, esclusivamente per finalità connesse all’operatività del sistema e della sicurezza. In questo caso, copie delle credenziali devono essere tenute, in modo da garantire la loro riservatezza, specificando, per iscritto, i soggetti responsabili del mantenimento di tali credenziali. Tali soggetti dovranno informare, senza indugio, l’incaricato delle attività svolte.

Controlli dell’accesso

20. Solo i Soggetti Autorizzati hanno accesso ai Dati Personali, anche quando memorizzati su qualsiasi supporto elettronico o portatile o quando vengono trasmessi. I soggetti Autorizzati sono abilitati esclusivamente all'accesso a quei dati e risorse necessari per poter svolgere le proprie mansioni.

21. I profili di autorizzazione per ciascun Soggetto autorizzato o per gruppi omogenei di Soggetti Autorizzati devono essere stabiliti e configurati prima dell'inizio di qualsiasi Trattamento in modo da abilitare il solo accesso ai dati e alle risorse che sono necessari, a ciascun Soggetto Autorizzato, per svolgere le proprie mansioni.

22. Viene verificata regolarmente, almeno con cadenza annuale, la sussistenza dei requisiti e delle condizioni per il mantenimento dei profili di autorizzazione per ciascun Soggetto Autorizzato. Ciò può comprendere anche l'elenco delle Persone Autorizzate redatto per categorie omogenee di attività e profilo di autorizzazione corrispondente.

23. Sono adottate misure per impedire l'accesso o l'uso dei Sistemi Informativi a persone non autorizzate. In particolare, firewall e sistemi anti-intrusione, aggiornati secondo lo stato dell'arte e le migliori prassi del settore, devono essere installati per proteggere i Sistemi Informativi da accessi non autorizzati. Sono adottate misure per accertare quando sono stati utilizzati i Sistemi Informativi o i Dati Personali sono stati Trattati senza autorizzazione, o quando vi siano stati tentativi di accesso o di trattamento dei dati non autorizzati che non siano andati a buon fine.

24. I controlli di accesso al sistema operativo o al database devono essere configurati correttamente per garantire solo accessi autorizzati.

25. Solo il personale autorizzato dal Responsabile, può concedere, modificare o annullare l'accesso autorizzato dai soggetti ai Sistemi Informativi.

Gestione dei supporti fisici

26. I Sistemi informativi e i supporti fisici di memorizzazione di dati personali devono essere conservati in un ambiente fisico sicuro. Devono essere adottate misure per impedire l'accesso fisico non autorizzato ai locali dei Sistemi Informativi.

27. Istruzioni organizzative e tecniche devono essere previste in relazione al mantenimento e all'utilizzo di supporti rimovibili su cui sono memorizzati i dati al fine di prevenire l'accesso e l'elaborazione non autorizzati.

28. I Supporti contenenti Dati Personali devono consentire di identificare e classificare il tipo di informazioni in essi contenuti (indicando la data di inserimento dei dati; l'utente autorizzato che ha inserito i dati e la persona da cui sono stati ricevuti i dati; i dati personali immessi); detti Supporti devono essere archiviati in un luogo con accesso fisico limitato al personale autorizzato.

29. Quando i Supporti devono essere smaltiti o riutilizzati, prima di procedervi devono essere adottate le misure necessarie per impedire qualsiasi conseguente reperimento di Dati Personali e altre informazioni su questi memorizzate, che le informazioni siano comprensibili o ricostruite con qualsiasi mezzo tecnico.

30. Il supporto contenente Dati Personali deve essere eliminato o reso illeggibile se non viene più utilizzato o prima di essere smaltito.

Distribuzione dei supporti e Trasmissione

31. I supporti contenenti Dati Personali devono essere disponibili solo ai Soggetti Autorizzati.

32. I Trattamenti di stampa/copia devono essere fisicamente controllati dai Soggetti autorizzati, per garantire che nessuna stampa o copia contenente Dati Personali rimanga in stampanti o fotocopiatrici.

33. I supporti contenenti Dati Personali o copie stampate di Dati Personali devono contenere la dicitura "Riservato".

34. La crittografia o altra forma equivalente di protezione deve essere utilizzata per proteggere i Dati Personali che sono elettronicamente trasmessi su una rete pubblica o memorizzati su un dispositivo portatile, o laddove si debbano conservare o trattare Dati Personali in un ambiente fisicamente insicuro.

35. I documenti cartacei contenenti Dati Personali devono essere trasferiti in un contenitore/busta sigillata che indica chiaramente che il documento deve essere consegnato a mano a un soggetto autorizzato a riceverli dal Titolare del trattamento.

36. Quando i Supporti contenenti Dati Personali devono essere trasferiti in locali designati a seguito di operazioni di manutenzione, devono essere adottate le misure necessarie per evitare qualsiasi recupero non autorizzato dei Dati Personali e delle altre informazioni sugli stessi memorizzati.

37. Deve essere istituito un sistema per la registrazione in entrata e in uscita dei Supporti che consenta l'identificazione diretta o indiretta del tipo di supporto, la data e ora, il mittente/destinatario, il numero di supporti, il tipo di informazioni contenute, come vengono inviati e la persona Responsabile per la loro ricezione/ invio, che deve essere debitamente autorizzata.

38. Qualora i Dati Personali siano trasmessi o trasferiti su una rete di comunicazione elettronica, devono essere messe in atto misure per controllare il flusso di dati e registrare i tempi della trasmissione o del trasferimento, i Dati Personali trasmessi o ceduti, la destinazione degli eventuali Dati Personali comunicati o trasferiti e i dettagli del Soggetto Autorizzato che conduce la trasmissione o il trasferimento.

Conservazione, copie di Back-up e recupero

39. Devono essere messi in atto strumenti per prevenire il deterioramento non intenzionale o la distruzione dei Dati Personali.

40. Devono essere definite e stabilite procedure per fare copie di back-up e di ripristino dei dati. Queste procedure devono garantire che i file di Dati Personali possono essere ripristinati nello stato in cui erano al momento della loro perdita o distruzione.

41. Devono essere effettuate copie di back-up almeno una volta a settimana, a meno che nessun dato sia stato aggiornato in quell'intervallo di tempo.

Rilevamento antivirus e intrusioni

42. Devono essere installati sui Sistemi Informativi software anti-virus e sistemi di rilevamento delle intrusioni per la protezione contro attacchi o altre attività non autorizzate sui Sistemi Informativi stesso. I software antivirus e i sistemi di rilevamento delle intrusioni devono essere aggiornati regolarmente secondo lo stato dell'arte e dell'industria esistenti per i Sistemi informativi interessati . Le interfacce utente web, esposte su internet, devono essere protette da web application firewall (WAF).

Aggiornamento Software

43. Il software, il firmware e l'hardware utilizzato nei Sistemi Informativi sono riesaminati regolarmente al fine di rilevare le vulnerabilità e le falle nei Sistemi stessi e di risolvere tali vulnerabilità e i difetti.

44. Deve essere previsto un processo di patching dei sistemi informativi volto a consentire l'implementazione in tempi rapidi delle patch di security e che preveda l'installazione sugli stessi sistemi del patch bundle più aggiornato con cadenza regolare e nel rispetto dello stato dell'arte del settore, in base ai sistemi operativi in uso.

Conservazione dei dati

Accesso fisico ai Dati

45. Solo il personale debitamente autorizzato dal Responsabile può avere accesso fisico ai locali dove vengono conservati i Sistemi informativi e i supporti di memorizzazione di Dati Personali. Deve essere mantenuto un registro del personale che accede a tali locali, che indichi il nome, la data e l'ora di accesso.

Documento degli incidenti

46. Deve esistere una procedura per la segnalazione, per la risposta e la gestione degli incidenti quali le violazioni della sicurezza dati o i tentativi di accesso non autorizzato.

47. Il Responsabile deve avvisare immediatamente il Titolare del trattamento nel caso in cui i Dati Personali siano stati coinvolti nell'incidente o nella violazione o potrebbero essere coinvolti o attaccati in qualche modo.

Audit

48. Regolari Audit sulla conformità a tali requisiti minimi di sicurezza devono effettuarsi con cadenza periodica.

Distribuzione dei Supporti

49. I Supporti contenenti Dati Personali possono essere distribuiti solo se i dati sono stati

crittografati per garantire che tali Dati Personali e altre informazioni non siano intelligibili o non possono essere manipolate in transito.

Recupero e copie di back-Up

50. Una copia di back-up deve essere tenuta in un luogo diverso da quello dei Sistemi Informativi; i presenti requisiti minimi di sicurezza si applicano a tali copie di back

Rete di comunicazione elettronica

51. I Dati Personali potranno essere diffusi tramite reti di comunicazioni elettroniche solo se essi sono stati crittografati, cifrati o è utilizzato un altro meccanismo per garantire che le informazioni non sono intellegibili o non siano manipolate da terzi.

Allegato 2
ISTRUZIONI PER IL RESPONSABILE ALLE OPERAZIONI DI TRATTAMENTO DEI DATI PERSONALI E PARTICOLARI

ATTIVAZIONE TESSERA SANITARIA

- dopo aver effettuato il riconoscimento de-visu del cittadino, lo invitate a leggere l'informativa per la tutela dei dati personali affissa presso lo sportello;
- accedete al Card Management System (CMS) identificandovi mediante la Vostra smart card, se non ancora operativi sul sistema;
- richiedete al cittadino di esprimere verbalmente la volontà di procedere con l'attivazione della carta e il consenso al trattamento dei dati personali;
- richiedete al cittadino la TS-CNS e la inserite nel lettore di smart card collegato al computer;
- eseguite una verifica dell'identità del cittadino confrontando i dati del documento di identità con i dati contenuti nel CMS;
- prendete una busta PIN pre-stampata a caso tra quelle assegnatevi e inserite sul CMS il codice della busta riportato esternamente leggendolo mediante il lettore di codice a barre o inserendo manualmente il numero corrispondente;
- utilizzate la specifica funzionalità del CMS, che accede al PUK della carta senza visualizzarlo e modifica il codice PIN della TS-CNS assegnandogli il valore contenuto nella busta;
- consegnate al cittadino la busta cieca contenente il codice PIN e il codice utente;
- ricevete l'eventuale modulo di richiesta del lettore di TS-CNS, che viene fornito gratuitamente dalla Regione Sardegna ad ogni nucleo familiare, consegnate il lettore al cittadino e registrate l'operazione sul CMS;
- consegnate al cittadino l'informativa relativa alle operazioni svolte.

Le modalità operative sopra descritte, se correttamente utilizzate, assicurano che nessuno, nemmeno Voi, possa conoscere il codice PIN, se non aprendo la busta cieca.

1. Sono previste procedure diverse per l'identificazione ed attivazione della TS-CNS in casi particolari, di seguito elencati; per ciascuna particolare tipologia si specificheranno esclusivamente le operazioni peculiari ed ulteriori necessarie, ferme restando le modalità operative descritte al punto 1 del presente documento.

a) Minori degli anni 18: in caso di TS-CNS intestata ad un minore l'identificazione verrà effettuata nei confronti del genitore, che dovrà presentarsi allo sportello con un proprio documento di identità valido. La presenza allo sportello del minore non è necessaria. Al genitore verrà richiesto di firmare una dichiarazione di autocertificazione della responsabilità genitoriale. Sulle TS-CNS intestate a minori non è consentita l'attivazione della firma digitale.
b) Minore emancipato: in caso di TS-CNS intestata ad un minore emancipato l'identificazione avverrà secondo la procedura standard descritta al punto 1 del presente documento. Inoltre il Titolare dovrà dare evidenza all'operatore del suo stato (esibizione di un documento di identità da cui risulti il matrimonio, copia dell'atto giuridico comprovante lo status di minore emancipato o apposita autocertificazione). Sulle TS-CNS intestate a minori emancipati non è consentita l'attivazione della firma digitale.

c) Incapaci legali di agire (interdetti, inabilitati e amministrati di sostegno): in caso di TS-CNS

intestata ad una persona sottoposta a tutela, curatela o amministrazione di sostegno l'identificazione verrà effettuata nei confronti del rappresentante legale, che dovrà presentarsi allo sportello con un proprio documento di identità valido. La presenza allo sportello della persona incapace legale di agire non è necessaria. Al rappresentante legale verrà richiesto di firmare una dichiarazione di autocertificazione del suo status. Sulle TS-CNS intestate a persone sottoposte a tutela non è consentita.

d) Nel caso in cui il Titolare non possa recarsi agli sportelli di attivazione per l'identificazione, è possibile procedere alla richiesta dei codici segreti per delega. Il delegato dovrà essere identificato secondo la procedura standard descritta al punto 1 del presente documento e dovrà inoltre portare con sé un documento di identità e una dichiarazione sostitutiva di atto di notorietà attestante l'impossibilità del delegante, a presentarsi di persona, sottoscritta dallo stesso delegante.

2. Prima di procedere a qualunque trattamento (compresa l'identificazione personale) relativo alla gestione del ciclo di vita della TS-CNS, dovete eseguire, ovvero assicurarvi che siano già stati eseguiti, gli adempimenti relativi all'informativa nei confronti dell'interessato (ai sensi dell'art. 13 e 14 del REG UE 679/2016).
   Potrete agevolmente fornire le suddette informazioni, oltre che in forma orale, in forma scritta mediante l'apposita informativa predisposta dal Titolare del trattamento da esporre in maniera visibile in farmacia.

3. In riferimento al trattamento dei dati particolari inerenti lo stato di salute del cittadino, non è necessaria l'acquisizione del consenso in quanto il REG UE 679/2016 consente il trattamento di dati sanitari senza richiedere il consenso del cittadino, qualora il trattamento sia effettuato per finalità di assistenza sanitaria e di terapia da parte di professionisti della salute, ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità e se i dati sanitari sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale, come ad esempio è il caso della farmacia la cui conduzione professionale è sempre affidata ad un farmacista (ai sensi dell'art. 9 comma 2 lett. h e comma 3, del REG UE 679/2016). Nondimeno la necessità di un puntuale consenso per l'istituzione, la consultazione e il cd pregresso è espressamente prescritta dall'art. 12 D.l. 179/2012 e dal DPCM 178/2015.

ATTIVAZIONE FASCICOLO SANITARIO ELETTRONICO

Per la registrazione del consenso all'attivazione del Fascicolo, l'operatore di farmacia esegue i seguenti semplici passi:

- rende disponibile mediante locandina affissa l'informativa privacy al cittadino che intende attivare il proprio fascicolo e lo invita alla sua lettura;
- procede alla sua autenticazione sulla Intranet Medir mediante CNS o SPID;
- digita il codice fiscale del cittadino;
- richiede verbalmente conferma al cittadino sull'invio dei (tre) consensi e spunta sui rispettivi campi di verifica;
- richiede conferma al cittadino circa la sua presa visione dell'informativa e spunta sul rispettivo campo di verifica;
- conclude la registrazione elettronica;
- stampa il riepilogo dell'operazione per la sottoscrizione da parte del cittadino;
- conserva il documento firmato in apposita scatola;

- fornisce all'utente che ne faccia richiesta copia del modulo sottoscritto, specificando altresì che, nella propria area personale, l'utente può sempre verificare data, ora e nominativo dell'operatore che ha registrato l'operazione di attivazione del FSE (o di modifica del consenso).

CONSULTAZIONE PRESCRIZIONI DEMATERIALIZZATE DAL FASCICOLO SANITARIO ELETTRONICO

Per la consultazione delle prescrizioni presenti sul Fascicolo Sanitario Elettronico del proprio cliente, finalizzata al veloce e agevole recupero del NRE, l'operatore di farmacia esegue i seguenti semplici passi:

- procede alla sua autenticazione sulla Intranet Medir mediante CNS o SPID;
- accede al menu "ricerca prescrizioni";
- digita il codice fiscale del cittadino;
- visualizza l'elenco delle prescrizioni dematerializzate del cittadino dal quale può scaricare quelle d'interesse o semplicemente copiare il NRE

Si precisa che quest'operazione è possibile solo se il cittadino ha preventivamente attivato il suo Fascicolo.

ALTRI SERVIZI DI CUI ALL'ART. 1 COMMA 2 DELLA CONVENZIONE PER L'EROGAZIONE DI SERVIZI ICT

PRESSO LE FARMACIE CONVENZIONATE" del 07/03/2017 tra la *Regione Autonoma della Sardegna* e *Federfarma*

La Farmacia in qualità di Responsabile esterno del trattamento dei dati deve mettere a disposizione del cittadino una postazione elettronica tramite la quale, eventualmente col supporto del personale incaricato al trattamento dei dati della Farmacia, il cittadino stesso possa, attraverso le proprie credenziali:

- accedere al proprio FSE e ritirare/stampare i referti;
- effettuare la scelta e revoca del medico;
- richiedere l'esenzione per reddito dal pagamento del ticket.

Allegato 3
DETTAGLIO DEI TRATTAMENTI

Denominazione trattamento: FSE

Finalità: cura, studio e ricerca, governo

Base giuridica: esecuzione compiti di interesse pubblico, di cui all'art. 6, comma 1, lett. e) del GDPR, affidati alla Regione Autonoma della Sardegna dalle disposizioni statutarie e in ottemperanza a quanto previsto dal D.L. 179/2012 e dal DPCM 178/2015; con particolare riferimento al trattamento dei dati contenuti nelle prescrizioni farmaceutiche relativamente alla finalità di cura la base giuridica è il consenso dell'interessato ai sensi dell'art. 12 D.L. 179/2012.

Processi di trattamento: assistenza all'utente; gestione consenso al caricamento dei documenti; consultazione; consultazione prescrizioni farmaceutiche e numero di ricetta elettronica della prescrizione erogata; consultazione prescrizioni farmaceutiche dematerializzate.

Categorie trattamento:

[X] raccolta

[X] registrazione

[X] conservazione

[X] consultazione

[X] Modifica

Categorie di dati personali trattati:

Dati personali identificativi (nome, cognome, codice fiscale, residenza)

Dati personali relativi alla situazione economica

Dati particolari inerenti lo stato di salute

Categorie di soggetti interessati:

Cittadini

Denominazione trattamento: TS-CNS/CMS.

Finalità: Attivazione della firma digitale e della carta nazionale dei servizi nella tessera sanitaria

Base giuridica: esecuzione compiti di interesse pubblico di cui all'art.6, comma 1, lett. e) del GDPR derivanti dalla legge 24 novembre 2003, n. 326 e ss.mm.ii. e del D.Lgs. n. 82/2005.

Processi di trattamento: assistenza all'utente; attivazione certificato TS-CNS; inserimento certificato di firma su TS-CNS

Categorie trattamento:

[X] registrazione

[X] consultazione

Categorie di dati personali trattati:

Dati personali identificativi (nome, cognome, data di nascita, codice fiscale, residenza)

Dati particolari inerenti lo stato di salute

Categorie di soggetti interessati:

Cittadini