MINISTERO DELL'ECONOMIA E DELLE FINANZE

DECRETO 3 giugno 2020

Modalita' tecniche per il coinvolgimento del Sistema tessera sanitaria ai fini dell'attuazione delle misure di prevenzione nell'ambito delle misure di sanita' pubblica legate all'emergenza COVID-19. (20A03083)

(GU n.144 del 8-6-2020)

IL RAGIONIERE GENERALE DELLO STATO
del Ministero dell'economia e delle finanze

di concerto con

IL SEGRETARIO GENERALE
del Ministero della salute

Visto l'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, e successive modificazioni ed integrazioni (Sistema tessera sanitaria);

Visto il decreto del Presidente del Consiglio dei ministri 26 marzo 2008, pubblicato nella Gazzetta Ufficiale n. 124 del 28 maggio 2008, attuativo del citato art. 50, comma 5-bis, concernente le modalita' tecniche per il collegamento telematico in rete dei medici del Servizio sanitario nazionale;

Visto l'art. 6 del decreto-legge 30 aprile 2020, n. 28, concernente il Sistema di allerta Covid-19, il quale, tra l'altro, prevede:

al comma 1, che al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanita' pubblica legate all'emergenza COVID-19, e' istituita una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile. Il Ministero della salute, in qualita' di titolare del trattamento, si coordina, anche per il tramite del Sistema tessera sanitaria, con le strutture pubbliche e private accreditate che operano nell'ambito del Servizio sanitario nazionale, nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica da COVID 19, per gli ulteriori adempimenti necessari alla gestione del sistema di allerta e per l'adozione di correlate misure di sanita' pubblica e di cura;

al comma 2, che il Ministero della salute, all'esito di una valutazione di impatto, costantemente aggiornata, effettuata ai sensi dell'art. 35 del regolamento (UE) 2016/679, adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le liberta' degli interessati, sentito il Garante per la protezione dei dati personali ai sensi dell'art. 36, paragrafo 5, del medesimo regolamento (UE) 2016/679 e dell'art. 2-quinquiesdecies del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;

al comma 6, che l'utilizzo dell'applicazione e della piattaforma,

nonche' ogni trattamento di dati personali effettuato ai sensi al presente articolo sono interrotti alla data di cessazione dello stato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020, ed entro la medesima data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi.

Considerato che il Ministero della salute, in qualita' di titolare del trattamento ai sensi del predetto art. 6, comma 1 del decreto-legge 30 aprile 2020, n. 28, designa il Ministero dell'economia e delle finanze quale responsabile esterno del trattamento dei dati di cui al presente decreto;

Visto il documento di valutazione di impatto di cui al citato art. 6, comma 2 del decreto-legge 30 aprile 2020, n. 28, il quale, tra l'altro, prevede:

i dati che l'operatore sanitario comunica tramite il Sistema tessera sanitaria alla piattaforma di cui al citato art. 6, comma 1 del medesimo decreto-legge 30 aprile 2020, n. 28;

la valutazione di impatto dei trattamenti effettuati nell'ambito del Sistema tessera sanitaria di cui al presente decreto;

Visto il decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni, concernente il Codice dell'amministrazione digitale;

Visto il regolamento n. 2016/679/UE del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);

Visto il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, concernente il Codice in materia di protezione dei dati personali, come modificato dal decreto legislativo 10 agosto 2018 n. 101, concernente «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»;

Acquisito il parere favorevole del Garante per la protezione dei dati personali n. 94 del 1° giugno 2020 espresso ai sensi dell'art. 36, paragrafo 4, del regolamento (UE) 2016/679;

Decreta:

Art. 1

Definizioni

1. Ai fini del presente decreto si intende per:

a) «Sistema TS», il sistema informativo di cui e' titolare il Ministero dell'economia e delle finanze in attuazione di quanto disposto dall'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326;

b) «Sistema di allerta Covid-19», il Sistema previsto dall'art. 6 del decreto-legge 30 aprile 2020, n. 28 costituito dalla applicazione mobile (App) e dalla componente di backend, la cui titolarita' e' del Ministero della salute;

c) «Codice OTP», il codice One time password di durata temporale limitata e in nessun modo riconducibile all'interessato;

d) «SAR», il Sistema di accoglienza regionale attraverso il quale gli operatori sanitari trasmettono i dati verso il Sistema TS;

e) «SSN», Sistema sanitario nazionale;

f) «operatore sanitario», l'operatore del Dipartimento di prevenzione della ASL autorizzato ad accedere al Sistema TS per la trasmissione al Sistema di allerta Covid-19 dei dati di cui al presente decreto;

g) «TEK», il Temporary exposure key, una chiave crittografica casuale generata da un telefono cellulare o altro dispositivo «mobile» dotato dell'App.

Art. 2

Trasmissione dei dati dagli operatori sanitari per il tramite del

Sistema TS

1. Il Sistema TS rende disponibili all'operatore sanitario, anche tramite SAR, le funzionalita' per la trasmissione dei dati per il Sistema di allerta Covid-19, secondo le modalita' di cui al presente articolo.

2. In caso di esito positivo di un tampone, l'operatore sanitario contatta il paziente per effettuare l'indagine epidemiologica, che prevede anche la verifica dell'installazione dell'App del Sistema di allerta Covid-19. Se il paziente ha installato l'App, gli sara' richiesto di aprirla e di utilizzare la funzione di generazione del codice OTP. Il paziente comunica i 10 caratteri del codice OTP all'operatore sanitario e attende l'autorizzazione a procedere con l'upload delle proprie TEK.

3. L'operatore sanitario, secondo le modalita' descritte nell'Allegato A che costituisce parte integrante del presente decreto, accede al Sistema TS, anche tramite SAR, con le credenziali in suo possesso e, in virtu' del particolare profilo attribuito, inserisce i dati forniti dal paziente concernenti:

a) il codice OTP comunicato dal paziente;

b) la data di inizio dei sintomi.

4. Il Sistema TS invia i dati di cui al precedente comma 3 al server di backend del Sistema di allerta Covid-19.

5. Gli errori di dettatura sono mitigati dalla presenza del check digit come ultimo carattere del codice OTP. Inoltre tale codice e' generato su un alfabeto di 25 caratteri che esclude le ambiguita' (il numero 0 e la lettera O ad esempio), ed in ogni caso e' sempre possibile procedere alla generazione di un nuovo codice.

6. Il Sistema TS rende disponibile il proprio portale www.sistemats.it per eventuali segnalazioni inerenti le sole funzionalita' del Sistema TS cui ai comma 3 e 4 del presente articolo.

7. Il Ministero della salute, in qualita' di titolare del trattamento ai sensi dell'art. 6, comma 1 del decreto-legge 30 aprile 2020, n. 28, designa il Ministero dell'economia e delle finanze quale responsabile esterno del trattamento dei dati di cui al presente decreto.

8. La valutazione di impatto dei trattamenti effettuati nell'ambito del Sistema tessera sanitaria di cui al presente decreto e' riportata nel documento di valutazione di impatto di cui all'art. 6, comma 2 del decreto-legge 30 aprile 2020, n. 28.

9. Le specifiche tecniche di cui al presente decreto saranno rese disponibili sul portale www.sistemats.it

Il presente decreto sara' pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 3 giugno 2020

Il Ragioniere generale
dello Stato
Mazzotta

Il Segretario generale
Ruocco

Allegato A

Modalita' di trasmissione dei dati dagli operatori sanitari
per il tramite del Sistema TS

Indice

sicurezza
3.3 Canali di comunicazione
3.4 Sistema di monitoraggio del servizio
3.5 Protezione da attacchi informatici
3.6 Sistemi e servizi di backup e disaster recovery
3.7 Sistema di log analysis applicativo
3.8 Accesso ai sistemi

1. Introduzione

Il presente allegato descrive le modalita' tecniche di trasmissione da parte degli operatori sanitari dei dati alla componente di backend del Sistema di allerta Covid-19, ai sensi dell'art. 2 comma 3 del presente decreto.

2. Servizio di invio del codice OTP

2.1 Descrizione del servizio

In riferimento all'art. 2 comma 2 del presente decreto, il servizio di invio dei dati al backend del Sistema di allerta Covid-19 attraverso il servizio descritto nel presente allegato.

2.2 Modalita' di fruizione

Il servizio di invio dei dati e' reso disponibile in modalita' applicazione web oppure in modalita' cooperativa tramite web services.

2.3 Accesso al servizio

Le possibilita' di accesso al servizio da parte dell'operatore sanitario sono riassunte nella seguente tabella, che esplicita gli utenti che possono accedere al sistema TS attraverso sistemi software con interfacce web o web services, oppure per il tramite di sistemi regionali (SAR).

ID	Utente	Modalita'	Autenticazione	Note
1	Operatore sanitario che accede tramite SAR	Web service tramite SAR	Autenticazione a 2 fattori, CNS, CIE, SPID	L'operatore sanitario si connette al sistema regionale che a sua volta invoca il servizio tramite client applicativo. Certificato di autenticazione rilasciato dal Sistema TS. Il codice fiscale dell'operatore viene trasmesso come campo applicativo nel tracciato. Il sistema regionale deve garantire i requisiti minimi di sicurezza adottati dal Sistema TS in termini di autenticazione forte, nel tracciato viene dichiarata la tipologia di autenticazione: 2 fattori, CNS, CIE, SPID.
			TS-CNS oppure CNS oppure basic authentication (ID utente e	L'operatore sanitario invoca il servizio tramite software gestionale.

			Web service tramite software gestionale	password) con pincode come fattore di autenticazione	Credenziali di autenticazione rilasciate dal Sistema TS.
2	Operatore sanitario				
					L'operatore sanitario invoca il servizio tramite interfaccia web.
				TS-CNS oppure CNS oppure basic authentication (ID utente e password) con pincode come fattore di autenticazione	Credenziali di autenticazione rilasciate dal Sistema TS.
3	Operatore sanitario	Applicazione web			

Tabella 1 - Modalita' di accesso

La modalita' 1 si rivolge alle regioni e alle Province autonome di Trento e Bolzano, che sono gli intermediari SAR che colloquiano con il Sistema TS e che permettono l'accesso all'operatore sanitario. L'operatore sanitario (utente finale) si autentica con il sistema regionale con credenziali e modalita' stabilite dalla regione; a sua volta la regione si autentica e coopera con il Sistema TS attraverso il servizio descritto nel presente allegato.

La modalita' 2 si rivolge al singolo operatore sanitario che tramite un software gestionale sviluppato ad hoc si connette al servizio utilizzando la propria TSCNS oppure le proprie credenziali rilasciate dal Sistema TS.

La modalita' 3 si rivolge al singolo utente che accede ad una applicazione web resa disponibile sul portale del Sistema TS utilizzando la propria TS-CNS oppure le proprie credenziali rilasciate dal Sistema TS.

Gli operatori sanitari del Sistema TS sono quasi tutti dotati di pincode, la percentuale che non ne e' dotata e' di circa l'8%.

Al fine di rinforzare le misure di sicurezza adottate dal Sistema TS, di seguito si riporta una sintesi degli interventi che saranno attuati e delle relative tempistiche:

in aggiunta alle normali credenziali (ID utente e password), assegnazione del pincode come ulteriore fattore di autenticazione a tutti gli utenti che ancora non ne sono dotati (entro sessanta giorni dalla data di adozione del decreto);

implementazione dell'autenticazione a 2 fattori con OTP temporaneo (entro novanta giorni dalla data di adozione del decreto);

introduzione delle asserzioni SAML per i sistemi regionali necessarie per l'autenticazione per l'accesso al Sistema TS (entro novanta giorni dalla data di adozione del decreto).

2.4 Tracciato del servizio

Di seguito si descrivono i messaggi di richiesta e di risposta del servizio, validi sia per la modalita' web che per la modalita' web service.

Messaggio di richiesta

Campo	Descrizione	Obbligatorio
Codice OTP	Codice One Time Password	SI
Data inizio sintomi	Data di inizio dei sintomi	SI

Messaggio di risposta

Campo	Descrizione	Fonte
Identificativo transazione	Identificativo alfanumerico della transazione, generato dal sistema	Sistema TS
	Data-ora-minuti-secondi-millisecondi in	Sistema

Data-ora	cui si e' conclusa la transazione	TS
		Backend App
Esito	Esito della transazione	Immuni

2.5 Registrazione degli accessi applicativi e tempi di conservazione

Il servizio non costituisce ne' alimenta alcuna banca dati contenuta nel Sistema TS, in quanto la sua finalita' e' la trasmissione dei dati al backend dall'App.

Il sistema registra unicamente gli accessi all'applicazione e l'esito dell'operazione, e inserisce i dati dell'accesso in un archivio dedicato. In nessun caso sono tracciati i dati applicativi (OTP, data inizio sintomi), ne' su banca dati ne' su file di log, ne' su altro mezzo.

Per ciascuna transazione effettuata saranno registrati i seguenti dati relativi all'accesso e all'esito dell'operazione.

Nel caso di utente che accede tramite SAR (punto 1 della Tabella 1): identificativo della regione che si autentica, codice fiscale dell'operatore sanitario, data-ora-minuti-secondi-millisecondi dell'accesso, operazione richiesta, esito della transazione, identificativo della transazione.

Nel caso di utente che accede tramite credenziali rilasciate dal sistema TS (punti 2 e 3 della Tabella 1): codice fiscale dell'operatore sanitario, data-oraminuti-secondi-millisecondi dell'accesso, operazione richiesta, esito della transazione, identificativo della transazione.

I log degli accessi cosi' descritti sono conservati per dodici mesi.

3. Misure di sicurezza

3.1 Infrastruttura fisica

L'infrastruttura fisica e' realizzata dal Ministero dell'economia e delle finanze attraverso l'utilizzo dell'infrastruttura del Sistema tessera sanitaria in attuazione di quanto disposto dal presente decreto.

I locali sono sottoposti a videosorveglianza continua e sono protetti da qualsiasi intervento di personale esterno, ad esclusione degli accessi di personale preventivamente autorizzato necessari alle attivita' di manutenzione e gestione tecnica dei sistemi e degli apparati.

L'accesso ai locali avviene secondo una documentata procedura, prestabilita dal titolare del trattamento, che prevede l'identificazione delle persone che accedono e la registrazione degli orari di ingresso ed uscita di tali persone.

3.2 Registrazione degli utenti ed assegnazione degli strumenti di sicurezza

E' presente una infrastruttura di Identity e Access Management che censisce direttamente le utenze, accogliendo flussi di autenticazione e di autorizzazione, per l'assegnazione dei certificati client di autenticazione, delle credenziali di autenticazione e delle risorse autorizzative.

L'autenticazione delle regioni verso il sistema avviene attraverso certificato client con mutua autenticazione. Il certificato viene emesso con un sistema di crittografia asimmetrica a chiave pubblica/privata.

Il sistema effettua la gestione completa del certificato di autenticazione: assegnazione, riemissione alla scadenza, revoca.

La gestione e la conservazione del certificato client sono di esclusiva responsabilita' del soggetto cui e' stato assegnato. L'autenticazione degli operatori sanitari avviene tramite TS-CNS oppure CNS oppure credenziali e pincode.

La TS-CNS e' prodotta e consegnata dal Sistema TS a tutti gli assistiti del SSN. La tessera e' dotata di chip che contiene il certificato di autenticazione personale. Prima del primo utilizzo come dispositivo di autenticazione, la tessera deve essere attivata presso il Card Management System della regione di riferimento.

Per l'autenticazione e' possibile anche utilizzare una CNS distribuita dai sistemi regionali.

Un ulteriore metodo di autenticazione per gli operatori sanitari e' costituito dalle credenziali dotate di pincode. L'assegnazione

delle credenziali agli utenti del Sistema TS e' effettuata dagli amministratori di sicurezza presenti in ciascuna ASL.

La registrazione degli operatori sanitari si effettua presso la ASL di riferimento che consegna le credenziali e la prima parte del pincode.

La seconda parte del pincode si ottiene direttamente sul portale del Sistema TS dopo la prima autenticazione.

La gestione dei profili di autorizzazione e' effettuata sempre dagli amministratori di sicurezza delle ASL. A tutti gli operatori sanitari che devono essere autorizzati viene assegnata una risorsa di autorizzazione creata e dedicata appositamente al servizio descritto dal presente decreto.

Gli amministratori di sicurezza si autenticano con le credenziali in basic authentication. Entro sessanta giorni dalla data di adozione del decreto saranno dotati di strumenti di autenticazione forte.

La gestione degli amministratori di sicurezza delle ASL e' effettuata dall'Amministratore centrale della sicurezza. L'Amministratore centrale della sicurezza e' nominato tra gli incaricati del trattamento.

3.3 Canali di comunicazione

Le comunicazioni sono scambiate in modalita' sicura su rete SPC per le regioni ovvero tramite Internet, mediante protocollo TLS in versione minima 1.2, al fine di garantire la riservatezza dei dati. I protocolli di comunicazione TLS, gli algoritmi e gli altri elementi che determinano la sicurezza del canale di trasmissione protetto sono continuamente adeguati in relazione allo stato dell'arte dell'evoluzione tecnologica, in particolare per il TLS non sono negoziati gli algoritmi crittografici piu' datati (es. MD5).

3.4 Sistema di monitoraggio del servizio

Per il monitoraggio dei servizi, il Ministero dell'economia e delle finanze si avvale di uno specifico sistema di reportistica.

3.5 Protezione da attacchi informatici

Per proteggere i sistemi dagli attacchi informatici al fine di eliminare le vulnerabilita', si utilizzano le seguenti tecnologie o procedure.

a) Aggiornamenti periodici dei sistemi operativi e dei software di sistema, hardening delle macchine.

b) Adozione di una infrastruttura di sistemi firewall e sistemi IPS (Intrusion Prevention System) che consentono la rilevazione dell'esecuzione di codice non previsto e l'esecuzione di azioni in tempo reale quali il blocco del traffico proveniente da un indirizzo IP attaccante.

c) Esecuzione di WAPT (Web Application Penetration Test), per la verifica della presenza di eventuali vulnerabilita' sul codice sorgente.

d) Adozione del captcha sull'applicazione web e di sistemi di rate-limit sui web services che limitano il numero di transazioni nell'unita' di tempo, al fine di mitigare il rischio di accesso automatizzato alle applicazioni che genererebbe un traffico finalizzato alla saturazione dei sistemi e quindi al successivo blocco del servizio.

3.6 Sistemi e servizi di backup e disaster recovery

Non sono previsti sistemi e servizi di backup e disaster recovery per i log di accesso in quanto non necessari per le finalita' di trattamento dei dati del servizio. Tali sistemi non sono previsti nemmeno per i dati, in quanto come gia' indicato nel par. 2.5 il sistema non registra nessun dato. Infatti, poiche' il sistema non prevede una banca dati e registra unicamente gli accessi al servizio, la perdita delle informazioni registrate non pregiudica ne' l'utilizzo ne' l'efficienza del servizio, in quanto il codice OTP ha durata limitata, non e' in alcun modo riconducibile all'interessato, e comunque puo' essere rigenerato in qualunque momento dal dispositivo «mobile» per poi essere trasmesso attraverso il servizio.

E' unicamente previsto il backup dei sistemi.

3.7 Sistema di log analysis applicativo

Non e' previsto un sistema di log analysis applicativo in quanto come indicato nel par. 3.6 non e' prevista la registrazione dei dati applicativi.

3.8 Accesso ai sistemi

L'infrastruttura dispone di sistemi di tracciamento degli accessi ai sistemi informatici di supporto come base dati, server web e

infrastrutture a supporto del servizio.

L'accesso alla base dati avviene tramite utenze nominali o riconducibili ad una persona fisica (escluse le utenze di servizio). Il sistema di tracciamento registra (su appositi log) le seguenti informazioni: identificativo univoco dell'utenza che accede, data e ora di login, logout e login falliti, postazione di lavoro utilizzata per l'accesso (IP client), tipo di operazione eseguita sui dati (ad esclusione delle risposte alle query).

Per ogni accesso ai sistemi operativi, ai sistemi di rete, al software di base e ai sistemi complessi (anche da parte degli amministratori di sistema), il sistema di tracciamento registra (su appositi log) le seguenti informazioni: identificativo univoco dell'utenza che accede, data e ora di login, logout e login falliti, postazione di lavoro utilizzata per l'accesso (IP client).

I log prodotti dai sistemi di tracciamento infrastrutturali sono soggetti a monitoraggio costante allo scopo di individuare eventuali anomalie inerenti alla sicurezza (accessi anomali, operazioni anomale, ecc.) e di valutare l'efficacia delle misure implementate.

I log di accesso degli Amministratori di sistema e degli incaricati sono protetti da eventuali tentativi di alterazione e dispongono di un sistema di verifica della loro integrita'. I log relativi agli accessi e alle operazioni effettuate sui sistemi operativi, sulla rete, sul software di base e sui sistemi complessi sono conservati per dodici mesi.