Allegato F:

MISURE DI SICUREZZA

Sommario

1. Premessa

Il presente allegato descrive le caratteristiche dell'infrastruttura e le misure adottate per garantire la riservatezza, l'integrità e la disponibilità dei dati trattati, nonché la sicurezza dell'accesso ai servizi, il tracciamento delle operazioni effettuate e assicurare che il trattamento dei dati sia effettuato in conformità ai principi di finalità del trattamento, di indispensabilità e necessità, di proporzionalità, pertinenza e non eccedenza dei dati personali trattati e nel rispetto delle disposizioni di cui al decreto legislativo 10 agosto 2018, n. 101, che ha adeguato il Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196) alle disposizioni di cui al Regolamento (UE) 2016/679 (GDPR).

L'infrastruttura è progettata, realizzata e gestita mettendo in atto misure tecniche e organizzative per soddisfare le norme citate (privacy by design) e per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (privacy by default).

2. Definizioni

a) **ASL:** Azienda Sanitaria Locale, unità territoriale che presta l'assistenza sanitaria ai cittadini;

b) **SAR:** Sistema di Accoglienza Regionale, attraverso il quale gli operatori sanitari invocano i servizi del sistema ANA;

c) **DGC:** Digital Green Certificate.

3. Accesso ai servizi e modalità di fruizione

Le possibilità di accesso ai servizi da parte delle varie tipologie di utenti sono riassunte nei seguenti paragrafi, suddivisi secondo le varie componenti del sistema indicate nell'articolo 4 del presente DPCM.

3.1 Raccolta dati

La raccolta dei dati avviene attraverso le funzionalità del Sistema TS.

Gli utenti e le modalità di connessione al Sistema TS sono descritti nell'allegato C del presente DPCM.

Nell'ottica del riutilizzo, la piattaforma nazione-DGC riutilizza l'infrastruttura per l'assegnazione degli strumenti di sicurezza del Sistema TS, in quanto già esistente e già conosciuta agli utenti (maggiori dettagli nel par. 5).

3.2 Generazione e conservazione delle certificazioni verdi

Il componente della raccolta dati trasferisce i dati necessari per la generazione delle certificazioni verdi al componente di generazione. Il colloquio è system-to-system ed avviene su canali di comunicazione che adottano le misure di sicurezza descritte nel par. 8.

3.3 Rilascio delle certificazioni verdi

Le modalità di messa a disposizione delle certificazioni verdi ai soggetti intestatari delle stesse sono descritte nell'allegato E.

Per quanto riguarda il frontend dedicato (sito web), le comunicazioni utilizzano canali che adottano le misure di sicurezza descritte nel par. 8.

Per quanto riguarda l'accesso al FSE, il cittadino e il medico MMG/PLS accedono secondo le modalità previste dalla normativa vigente, così come accade per gli altri documenti del FSE.

Per quanto riguarda la comunicazione tra le app e i servizi di backend dedicati, messi a loro disposizione, le comunicazioni utilizzano canali che adottano le misure di sicurezza descritte nel par. 8. Inoltre, il chiamante presenta un certificato di autenticazione (c.d. mutua autenticazione).

Per quanto riguarda l'accesso degli operatori al Sistema TS per il recupero come intermediario della certificazione verde COVID-19, le modalità sono descritte nell'allegato C del presente DPCM.

3.4 Utilizzo e verifica delle certificazioni verdi

L'app Verifier effettua la verifica in modalità *offline*, non sono quindi previste connessioni verso sistemi esterni in questa fase. L'unico collegamento è con i servizi previsti per l'interoperabilità europea che sono operanti in mutua autenticazione.

4. Infrastruttura di sicurezza

Al fine di garantire le adeguate misure di sicurezza, l'infrastruttura del Sistema TS è dotata delle seguenti componenti:

- infrastruttura di Identity & Access Management per l'identificazione dell'utente, la gestione dei profili autorizzativi, la verifica dei diritti di accesso, il tracciamento delle operazioni; nell'ottica del riutilizzo, tale infrastruttura è la stessa del Sistema TS in quanto già esistente e già conosciuta agli utenti;

- amministratori di sicurezza delle ASL: sono gli operatori che censiscono gli utenti e distribuiscono gli strumenti di sicurezza; anche in questo caso si utilizzano gli amministratori di sicurezza del Sistema TS già presenti e operativi sul territorio delle singole ASL;
- Certification Authority;
- sistema di monitoraggio dei servizi;
- sistema di log analysis;
- sistemi di sicurezza per la protezione delle informazioni e dei servizi;
- sistema di Disaster Recovery della banca dati;
- sistemi e servizi di backup per il salvataggio dei dati e delle applicazioni;
- infrastruttura per la registrazione degli accessi ai sistemi e alla base dati.

Nei seguenti paragrafi sono descritte le misure di sicurezza e le procedure che utilizzano i vari componenti.

5. Registrazione degli operatori sanitari ed assegnazione degli strumenti di sicurezza

L'infrastruttura di Identity e Access Management censisce direttamente le utenze, accogliendo flussi di autenticazione e di autorizzazione, per l'assegnazione dei certificati client di autenticazione, delle credenziali di autenticazione a 2 fattori e delle risorse autorizzative.

L'autenticazione delle regioni e verso il sistema avviene attraverso certificato client con mutua autenticazione. Il certificato viene emesso dalla Certification Authority con un sistema di crittografia asimmetrica a chiave pubblica/privata. Il sistema effettua la gestione completa del certificato di autenticazione: assegnazione, rinnovo alla scadenza, revoca. La gestione e la conservazione del certificato client sono di esclusiva responsabilità del soggetto cui è stato assegnato.

L'autenticazione degli operatori sanitari avviene tramite TS-CNS oppure CNS oppure con credenziali + pincode. La TS-CNS è prodotta e consegnata dal Sistema TS a tutti i cittadini che sono iscritti al SSN. La tessera è 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 è possibile anche utilizzare una CNS distribuita dai sistemi regionali. Un ulteriore metodo di autenticazione, per gli operatori sanitari, è costituito dalle credenziali di autenticazione e pincode, come ulteriore fattore rafforzativo. L'assegnazione delle credenziali agli utenti del

sistema è effettuata dagli amministratori di sicurezza del Sistema TS presenti in ciascuna ASL, con le modalità già in uso nel Sistema TS.

La registrazione degli operatori sanitari si effettua presso la ASL di riferimento, che gli consegna le relative credenziali di autenticazione.

La gestione dei profili di autorizzazione è 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 ai singoli servizi descritti nel presente decreto.

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

6. Registrazione degli accessi e tempi di conservazione

Per quanto riguarda l'accesso al Sistema TS, i dati degli accessi registrati e i tempi di conservazione sono indicati nell'allegato C.

Per quanto riguarda l'accesso al sito dedicato da parte del cittadino, il tracciamento viene effettuato dal backend (PN-DGC) e i dati conservati sono:

- codice fiscale, canale di accesso, modalità di autenticazione, data-ora dell'accesso, esito operazione, tipologia di certificato recuperato e tipologia di codice univoco nazionale associato al tipo di evento sanitario.

Il sistema registra gli accessi ai servizi e l'esito dell'operazione, e inserisce i dati dell'accesso in un archivio dedicato. Tali registrazioni sono usate ai soli fini della verifica della liceità del trattamento e per garantire l'integrità e la riservatezza dei dati personali.

I log degli accessi sono conservati in forma individuale fino al termine della validità delle relative certificazioni verdi COVID-19 a cui si riferiscono. Successivamente sono conservati in forma anonima e aggregata per le finalità degli analystics.

7. Infrastruttura fisica

L'infrastruttura fisica è 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 del personale preventivamente autorizzato, necessari alle attività 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.

8. Canali di comunicazione

Tutte le comunicazioni sono scambiate in modalità sicura 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 più datati (es. MD5).

Le regioni comunicano a scelta su rete SPC ovvero su rete Internet.

Tutte le altre comunicazioni avvengono su rete Internet.

9. Sistema di monitoraggio dei servizi

Per il monitoraggio del raggiungimento delle finalità normativamente previste per il servizio e per la diffusione delle informazioni rilevanti a fini di trasparenza, il Ministero della Salute, in qualità di titolare del trattamento dei dati della PN-DGC, e il Ministero dell'Economia e delle Finanze, responsabile del trattamento dei dati, si avvalgono di uno specifico sistema di reportistica. Il sistema offre funzioni per visualizzare i dati aggregati come il numero di vaccinazioni, tamponi e certificati di guarigione trasmessi al Sistema TS, ed anche il numero dei certificati verdi COVID-19 generati dalla piattaforma nazionale-DGC e acquisiti dagli interessati attraverso i diversi canali di messa a disposizione con le diverse modalità di autenticazione previste.

L'aggregazione può essere fatta per regione di assistenza, sesso, fascia d'età ed anche per intervallo temporale.

10. Sistema di log analysis

Sogei Spa, in qualità di responsabile del trattamento dei dati, adotta un sistema di log analysis per l'analisi periodica delle informazioni registrate nei log, in grado di individuare, sulla base

di regole predefinite e formalizzate e attraverso l'utilizzo di indicatori di anomalie (alert), eventi potenzialmente anomali che possano configurare trattamenti illeciti.

Sulla base di quanto monitorato dal sistema di log analysis, vengono generati, periodicamente, report sintetici sullo stato di sicurezza del sistema (es. accessi ai dati, rilevamento delle anomalie, etc.).

11. Protezione da attacchi informatici

Per proteggere i sistemi dagli attacchi informatici al fine di eliminare le vulnerabilità, 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 vulnerabilità sul codice sorgente.

d) Adozione del captcha sull'applicazione web senza accesso con identità digitale, e di sistemi di rate-limit sui web services che limitano il numero di transazioni nell'unità 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.

12. Disaster recovery e backup

È previsto il disaster recovery delle banche dati, sia per l'acquisizione dati su Sistema TS, sia per i certificati verdi COVID-19 sulla piattaforma nazione-DGC.

È previsto il backup periodico dei dati e dei sistemi.

13. Accesso ai sistemi

L'infrastruttura dispone di sistemi di tracciamento degli accessi ai sistemi informatici di supporto come sistemi operativi, server web e altre infrastrutture a supporto dei servizi.

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 integrità. 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.

14. Accesso alla base dati

L'infrastruttura dispone di un sistema di tracciamento degli accessi alla base dati.

L'accesso alla base dati, ove presente, 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).

I log relativi agli accessi alla base dati sono conservati per dodici mesi.