ALLEGATO *B*

1 Obiettivi del documento

Il presente Allegato individua le misure di sicurezza di cui all'articolo 27 del presente decreto, in conformità alle disposizioni degli articoli 25 e 32 del regolamento generale sulla protezione dei dati personali GDPR (UE n. 2016/679).

2 Misure di sicurezza per la protezione dei dati

Il Ministero della salute, le regioni e province autonome assicurano il rispetto delle disposizioni di cui all'articolo 51 del CAD in materia di sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni, nonché delle linee guida rese disponibili da AGID in materia di sviluppo e gestione dei sistemi informativi e di misure minime di sicurezza ICT per le pubbliche amministrazioni (CIRCOLARE AGID 18 aprile 2017, n. 2/2017), da attuare a livello avanzato.

Il Ministero della salute, le regioni e province autonome assicurano altresì la conformità al regolamento generale sulla protezione dei dati personali GDPR (UE n. 2016/679), con particolare riferimento all'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, ai sensi delle disposizioni di cui all'articolo 32, nonché al regolamento eIDAS per le interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni (UE n° 910/2014).

Il Ministero della salute, le regioni e province autonome adempiono alle misure previste dalla direttiva Network and Information Security (UE n° 1148/2016) e dalla direttiva Network and Information Security 2 (UE n° 2555/2022) e, per gli eventuali sotto-sistemi che dovessero ricadervi, alle misure previste dal perimetro nazionale di sicurezza cibernetica (DPCM 30 luglio 2020, n. 131).

L'infrastruttura del FSE è progettata, realizzata e gestita mettendo in atto misure tecniche e organizzative adeguate a 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).

Il Ministero della salute, le regioni e province autonome, per quanto di competenza, assicurano che anche i soggetti alimentanti il FSE adottino misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, ai sensi delle disposizioni di cui all'articolo 32 del GDPR.

Nei paragrafi che seguono si dettagliano le misure di sicurezza minime che il Ministero della salute, le regioni e province autonome devono assicurare.

2.1 Infrastruttura di sicurezza

Al fine di garantire le adeguate misure di sicurezza, tutti gli FSE regionali adottano le seguenti componenti:

- infrastruttura di Identity & Access Management (IAM) per l'identificazione dell'utente, la gestione dei profili autorizzativi, la verifica dei diritti di accesso, il tracciamento delle operazioni; la componente IAM permetterà l'accesso secondo le modalità previste (TS-CNS rilasciata dal Sistema TS, SPID livello 2 rilasciato dagli Identity Provider accreditati, CIE rilasciata dal Ministero dell'Interno, credenziali di autenticazione a 2 fattori rilasciate dal FSE), assicurando l'accesso alle sole risorse per le quali è permesso accedere
- infrastruttura di Privileged Access Manager, specifica per l'ecosistema ospitante il FSE, per la identificazione degli amministratori, la verifica dei privilegi di accesso alle risorse (Applicative, infrastrutturali, etc.,) ed il tracciamento delle attività svolte; la piattaforma è integrata con la componente IAM e implementa requisiti di accesso specifici (autenticazione forte tramite smart card o metodi equivalenti) per gli accessi amministrativi;

- Certification Authority: il FSE implementa un modello ibrido per quanto concerne l'adozione di certificati digitali, prevedendo sia una componente interna (adottatati per le comunicazioni intra FSE) che integrata con CA Esterne per quanto riguarda il riconoscimento di Certificati Digitali adottati dagli operatori delle PA abilitatati all'accesso al FSE. La CA Interna include la gestione delle chiavi private (Key Management Service) tramite l'adozione di sistemi di HSM;
- Componente di verifica dello stato dei servizi: il FSE prevede una componente centralizzata che provvede al monitoraggio relativo alla disponibilità e performance dei servizi erogati;
- Sistema di log analysis centralizzato per la raccolta degli eventi di sicurezza dalle componenti del FSE (componenti di sicurezza, server, Database, etc.) su cui sono disponibili Use Cases per il triage degli eventi ed il riconoscimento di possibili minacce/attacchi in corso e la consolle di Monitoraggio ad uso dell'unità organizzativa preposta alla gestione della sicurezza operativa (es. SOC).;
- Piano di continuità operativa: l'insieme coordinato dei processi e delle procedure di gestione Emergenza/Crisi ed attivazioni delle soluzioni di continuità operativa; il piano include i risultati della BIA/RA (aggiornati regolarmente) ed il piano dei Test periodici;
- Sistema di Disaster Recovery: l'insieme delle soluzioni tecniche/procedurali volte ad assicurare la continuità dei servizi erogati (per esempio Alta Affidabilità, Gestione delle Repliche, Scalabilità, infrastruttura speculare delle infrastrutture/dati);
- Sistemi e servizi di backup per il salvataggio dei dati e delle applicazioni: le componenti tecnologiche del FSE (sia in termini infrastrutturali, applicative e basi dati) sono integrate con componenti centralizzate di Backup e sistemi per la gestione delle repliche, e prevedono test periodici di Restore utili a verificare l'integrità dei dati salvati e la ricostruibilità degli ambienti operativi.

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

2.2 Sistema di autenticazione e autorizzazione degli utenti

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.

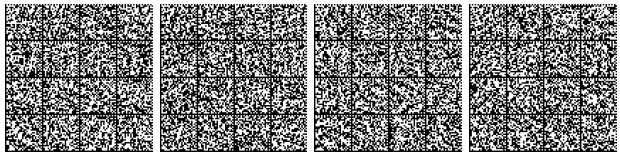
L'autenticazione dei sistemi terzi verso il FSE avviene attraverso certificato client con mutua autenticazione. Il certificato viene emesso dalla Certification Authority con un sistema di crittografia asimmetrica a chiave pubblica/privata. Il sistema effettua la gestione completa del certificato di autenticazione: assegnazione, rinnovo alla scadenza, revoca. La gestione e la conservazione del certificato client sono di esclusiva responsabilità del soggetto cui è stato assegnato. La CA del FSE provvede a gestire i certificati per la mutua autenticazione dei server che, laddove previsti, i certificati digitali per gli accessi in modalità di autenticazione forte; la CA permette l'utilizzo di Certificati Pubblici per i servizi/server esposti.

La gestione dei profili di autorizzazione è effettuata sempre dagli amministratori di sicurezza; l'accesso da parte degli amministratori avviene tramite la componente IAM e PAM (precedentemente descritte).

Gli amministratori di sicurezza si autenticano alle funzioni a loro dedicate con metodi di autenticazione forte.

L'Amministratore della sicurezza è nominato tra gli incaricati del trattamento.

L'infrastruttura IAM non permette a nessun utente di effettuare accessi multipli contemporanei utilizzando le proprie credenziali.



2.3 Registrazione degli accessi e tempi di conservazione ai fini della sicurezza

Il FSE registra gli accessi ai servizi e l'esito dell'operazione (sia accessi con esito positivo che negativo), e inserisce i dati dell'accesso in un archivio dedicato. Per ciascuna transazione effettuata sono registrati i seguenti dati minimi relativi all'accesso e all'esito dell'operazione:

- identificativo del sistema terzo che si autentica;
- codice fiscale dell'utente;
- ruolo dell'operatore;
- data-ora-minuti-secondi-millisecondi dell'accesso;
- operazione richiesta;
- esito dell'operazione;
- identificativo della transazione.

I log così descritti sono conservati per almeno dodici mesi.

2.4 Infrastruttura fisica

Le componenti tecnologiche del FSE sono dislocate presso Sale Dati e dotati di sistemi di segregazione Fisica; i locali tecnici sono sottoposti a videosorveglianza continua e sono protetti da qualsiasi intervento di personale esterno, ad esclusione degli accessi di 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 e periodicamente rivista, che prevede la preventiva autorizzazione del personale, l'identificazione delle persone che accedono e la registrazione degli orari di ingresso e uscita di tali persone.

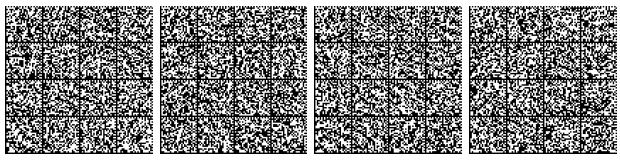
2.5 Canali di comunicazione

Tutte le comunicazioni tra le componenti del FSE avvengono in modalità sicura mediante protocollo TLS in versione minima 1.2, al fine di garantire la riservatezza dei dati e in conformità alle Raccomandazioni AGID in merito allo standard Transport Layer Security (TLS), adottate con Determinazione n. 471 del 5 novembre 2020. 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).

Tutte le altre comunicazioni avvengono su rete Internet.

2.6 Sistema di monitoraggio dei servizi

Per il monitoraggio dei servizi, la Regione si avvale di specifici sistemi di verifica del funzionamento dei sistemi (cosiddette "sonde" di monitoraggio) e di uno specifico sistema di reportistica. Il sistema di reportistica offre funzioni per visualizzare i dati aggregati come il numero di transazioni effettuate, viste come una qualunque sequenza di operazioni lecite, che, se eseguite in modo corretto, produce una variazione nello stato di una base di dati e relativi esiti. L'aggregazione può essere fatta per ASL o struttura che effettua la transazione. La finalità è di fornire il monitoraggio dell'andamento dei servizi.



2.7 Sistema di log analysis

La Regione 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. Il sistema di Log Analysis raccoglie e storicizza gli eventi di sicurezza ed analizza, tramite specifici meccanismi di correlazione degli eventi, eventuali anomalie o incidenti di sicurezza e fornisce in tempo reale tali segnalazioni sulla consolle di Monitoraggio ad uso dell'unità organizzativa preposta alla gestione della sicurezza operativa (es. SOC).

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.).

2.8 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 (patching e update)

b) Hardening delle macchine

c) separazione/segmentazione fisica o virtuale delle reti e l'isolamento delle risorse critiche

d) 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; l'infrastruttura FW è altresì integrata alla componente del NAC (Network Access Control) al fine di verificare l'adeguato livello di sicurezza degli End Point;

e) Adozione di sistemi WAF per il controllo del traffico applicativo;

f) Adozione di sistemi di AntiDDOS in grado di rilevare eventuali minacce/attacchi volumetrici ed implementare meccanismi di recovery;

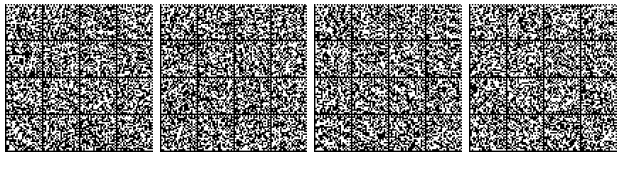
g) Server Protection – I server su cui sono attive le componenti del FSE implementano soluzioni di Extended Detection and Response (XDR) configurati per abilitare servizi di protezione avanzati (ad es. hunting, anti-ransomware, data loss prevention, etc.) per potenziare le capacità di rilevazione e risposta a potenziali attacchi cibernetici;

h) Esecuzione di periodici WAPT (Web Application Penetration Test), per la verifica della presenza di eventuali vulnerabilità sulle componenti del FSE.

2.9 Continuità operativa, disaster recovery e backup

Per il FSE viene definito il piano di continuità operativa che esplicita le procedure relative ai sistemi e ai servizi di backup e di Disaster Recovery. Nel piano sono riportati sia i risultati dalla Business Impact Analysis che gli scenari di crisi identificati e le procedure operative di gestione e reazione alla crisi ed i criteri per il calcolo dei tempi di ripristino. Il piano è sottoposto a test periodici, ed è aggiornato periodicamente per adeguarlo allo stato dell'arte della tecnologia disponibile ed al contesto operativo di riferimento, anche in relazione all'esito dei test svolti.

La procedura per la gestione dei backup dei dati definisce la frequenza con cui devono essere eseguiti i backup (almeno giornaliero), i test e le verifiche sul ripristino dei dati, le modalità di conservazione e la relativa retention (almeno 3 copie, conservate in non meno di due locazioni distinte e prevedendo una copia off-line - copia certificata dalla quale ripartire in caso di eventi malevoli/emergenze - es. attacco ransomware), nonché le modalità di cancellazione sicura ed irreversibile (nel caso in cui questo non sia possibile i supporti devono essere distrutti o resi inutilizzabili).



2.10 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.

2.11 Accesso alla base dati

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

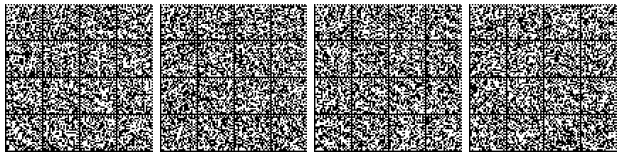
L'accesso alla base dati avviene tramite utenze nominali o riconducibili ad una persona fisica (escluse le utenze di servizio). Il sistema di tracciamento registra (su appositi log) le seguenti informazioni:

- 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).

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

Gli accessi alle basi dati sono inoltre sotto il monitoraggio della componente di DataBase Monitoring che esegue una verifica di tutte le connessioni al DB per verificarne la liceità e la correttezza.

La base dati del FSE è sottoposta ad un audit interno di sicurezza con cadenza periodica (almeno annuale), al fine di verificare l'adeguatezza delle misure di sicurezza.



2.12 Sistemi di protezione dei Dati

Le basi dati del FSE prevedono le seguenti misure:

- per i metadati, la cifratura dei dati idonei a rivelare lo stato di salute e la vita sessuale o la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali ;
- per i documenti, la cifratura degli stessi;
- i canali di comunicazione sono cifrati e mutuamente autenticati per l'accesso a dati personali (comuni e sensibili) 'in motion'.

Ai sensi dei commi 2 e 3 dell'articolo 17, per i trattamenti per le finalità di prevenzione effettuati dagli Uffici della Direzione generale del Ministero della salute competente in materia di prevenzione sanitaria e dagli Uffici delle Regioni e Province Autonome competenti in materia di prevenzione, il codice identificativo dell'assistito presente nei metadati viene sostituito da un codice univoco generato con un algoritmo di hash che, applicato al codice identificativo (dato in input), produce un codice univoco (digest di output) dal quale non è possibile risalire al codice identificativo di origine.

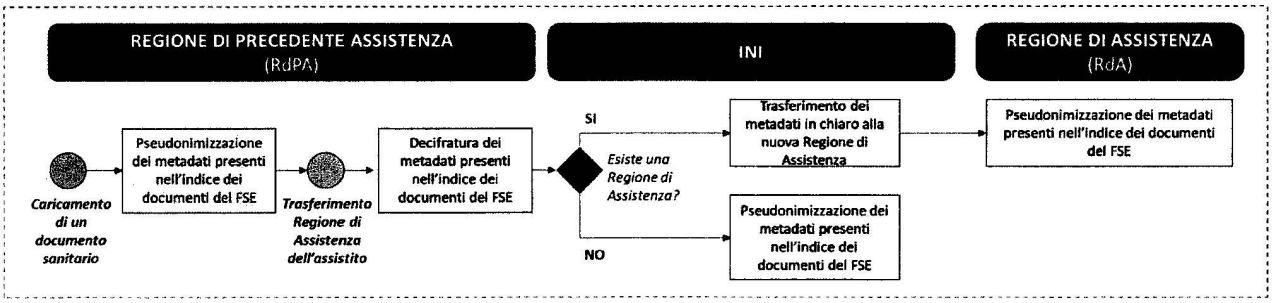
L'algoritmo di hash adottato è definito autonomamente da ogni Regione e Provincia Autonoma ed è diverso dall'algoritmo adottato ai sensi delle disposizioni di cui al decreto 7 dicembre 2016, n. 262. Gli archivi che contengono la decifratura autorizzata della pseudonimizzazione sono protetti con tecniche crittografiche adeguate allo stato dell'arte.

La funzione di hash dipenderà da una chiave di lunghezza adeguata alla dimensione e al ciclo di vita dei dati.

Ai sensi del comma 4 dell'articolo 17, per i trattamenti per le finalità di prevenzione effettuati dalla Direzione generale del Ministero della salute competente in materia di prevenzione sanitaria, il codice identificativo dell'assistito presente nei metadati viene sostituito da un codice univoco generato con un algoritmo che, applicato al codice identificativo, produce un codice univoco, un algoritmo che non consente l'identificazione diretta dell'interessato, ferma restando la possibilità di procedere all'identificazione dell'assistito ai fini del successivo accesso ai documenti del FSE dello stesso, ai sensi del comma 5 dell'articolo 17.

L'efficacia delle predette tecniche di pseudonimizzazione viene costantemente verificata tenendo conto dell'evoluzione dello stato dell'arte tecnologico anche alla luce delle raccomandazioni e delle linee guida via via adottate a livello europeo e a livello internazionale.

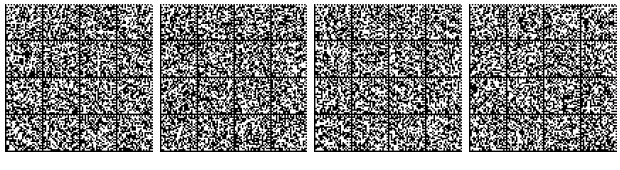
Per il trasferimento di assistenza, la Regione di precedente assistenza (RdPA) provvede a rendere disponibili, tramite INI, l'indice e i relativi metadati in chiaro alla Regione di nuova assistenza (RdA) la quale provvede autonomamente ad applicare le tecniche di pseudonimizzazione sopra indicate. Nel caso di mancanza di RdA, l'indice e i relativi metadati sono archiviati da INI che provvede ad applicare le tecniche di pseudonimizzazione sopra indicate.



2.13 Misure organizzative

Per il FSE sono assicurate le seguenti misure organizzative, in coerenza e a garanzia dell'efficacia ed efficienza delle misure di sicurezza tecnologiche indicate nei paragrafi precedenti:

- è verificata l'applicazione dei principi di data protection by default/design da parte dei produttori, nelle fasi di progettazione e sviluppo delle soluzioni FSE in conformità al Considerando 78 del Regolamento (cfr. EDPB - Linee Guida 4/2019 Data Protection by Design and by Default);
- sono adottate e verificate policy e procedure finalizzate a garantire che lo sviluppo delle soluzioni FSE avvenga nel rispetto di linee guida di secure coding conformi alle best practices (quali, a esempio, OWASP), anche con riferimento al costante controllo, identificazione e sostituzione delle librerie di terze parti che presentino vulnerabilità tali da determinare criticità nel trattamento dei dati;
- sono adottate e manutenute periodicamente procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento, anche con riferimento ai rischi di omonimia derivanti da bug software, errori di transcodifica o associazione dei metadati ai documenti, nei colloqui tra le varie componenti dei sistemi con particolare attenzione ai test di integrazione delle componenti e dei servizi (es. servizi di marcatura temporale dei documenti, chiamate ai web services, predisposizione di file XML per la trasmissione dei documenti, processi di firma multipla dei documenti sanitari);
- i profili di autorizzazione delle singole utenze o dei gruppi sono definiti sulla base dei principi del "*need to know*" e "*segregation of duties*" (si vedano in paragrafi 3 e 4 dell'Allegato A) e in particolare, anche ai fini della riduzione del rischio di re-identificazione:
    a. ai soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali e gli esercenti le professioni sanitarie che prendono in cura l'assistito sono attribuiti profili di autorizzazione che consentono esclusivamente il trattamento di dati personali per finalità di cura e prevenzione,
    b. agli Uffici delle Regioni e delle Province autonome competenti in materia di prevenzione sanitaria sono attribuiti profili di autorizzazione che consentono esclusivamente il trattamento di dati personali per finalità di prevenzione,
    c. alla Direzione generale del Ministero della salute competente in materia di prevenzione sanitaria sono attribuiti profili di autorizzazione che consentono esclusivamente il trattamento di dati personali per finalità di prevenzione;
    d. alla Direzione generale del Ministero della salute competente in materia di profilassi internazionale sanitaria sono attribuiti profili di autorizzazione che consentono esclusivamente il trattamento di dati personali per finalità di profilassi internazionale;
- le istruzioni, alle quali il personale deve attenersi per assicurare la tutela dei dati personali secondo i requisiti previsti dalla normativa vigente, sono integrate con l'ambito della sicurezza delle informazioni, riviste periodicamente e comunicate a tutto il personale interessato;
- le istruzioni, alle quali il personale deve attenersi, prevedono che i dati e i documenti sanitari e socio-sanitari soggetti a maggiore tutela dell'anonimato nascano oscurati e siano leggibili solo su specifica richiesta dell'interessato;
- in fase di stampa/download, il sistema avverte l'operatore del fatto che l'operazione comporta rischi di impropria esposizione dei dati dell'assistito, sottolinea il profilo di responsabilità e ricorda gli obblighi legati al trattamento dei dati;
- con le istruzioni impartite alle persone autorizzate al trattamento è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo della persona autorizzata;
- viene regolarmente svolta la formazione su specifiche tecnologie e componenti informatici con particolare attenzione alla sicurezza delle informazioni, per il personale responsabile della gestione di tali sistemi. I risultati dei percorsi formativi vengono registrati e riesaminati allo scopo di colmare eventuali lacune,



accrescere la sensibilizzazione e la cultura sui temi di sicurezza delle informazioni e gestione dei rischi, promuovere la comprensione delle politiche e delle procedure aziendali e favorire l'apprendimento dell'uso delle soluzioni/tecnologie di sicurezza;

- Per l'accesso alle prestazioni sanitarie viene utilizzato un lettore di codice a barre per leggere il codice identificativo dell'assistito dalla Tessera Sanitaria. Qualora ciò non sia possibile (ad esempio se la postazione è priva di lettore di codice a barre, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'assistito), le funzionalità per l'inserimento del codice identificativo dell'assistito, non prevedono funzionalità di auto completamento. In ogni caso il dato inserito viene verificato con l'Anagrafe Nazionale Assistiti che restituisce gli altri dati identificativi dell'assistito, anche al fine di permettere una ulteriore verifica della corretta identificazione dell'assistito da parte dell'operatore.
- Per assicurare la riduzione dei rischi per erroneo inserimento/associazione/attribuzione dei dati identificativi dell'assistito:
    a. l'identità dell'assistito viene verificata ad ogni passaggio del percorso assistenziale da parte degli operatori;
    b. la corrispondenza tra i metadati anagrafici dell'assistito del documento, i dati identificativi dell'assistito presenti nel documento e l'identificativo dell'assistito cui si riferisce il FSE viene verificata durante tutte le elaborazioni e nella fase di alimentazione del FSE;
- Per assicurare il rispetto dell'oscuramento dei documenti, con particolare riferimento ai dati e i documenti sanitari e socio-sanitari soggetti a maggiore tutela dell'anonimato:
    a. il documento oscurato viene identificato con un apposito attributo tra i metadati;
    b. l'attributo di oscuramento viene sempre verificato da tutte le procedure che agiscono sui documenti (es. ricerca. accesso, …);
    c. il documento oscurato non viene mai restituito in risposta alle transazioni di ricerca dei documenti.
- sono adottate e manutenute periodicamente procedure che indicano riferimenti per la segnalazione degli eventi di sicurezza delle informazioni nei sistemi informativi da parte di dipendenti, consulenti o addetti terzi prevedendo appositi canali gestiti per riportare incidenti nel più breve tempo possibile;
- è adottata e manutenuta periodicamente una procedura di gestione degli incidenti (inclusi i data breach) che definisce le risorse e le responsabilità delle persone che devono intervenire nella classificazione, risoluzione e gestione dell'incidente di sicurezza, ivi incluse le terze parti (es. fornitori di soluzioni tecnologiche, fornitori di servizi di assistenza e manutenzione);
- i contratti di esternalizzazione di servizi a fornitori/terze parti (c.d. outsourcing) specificano il ruolo di tali fornitori/terze parti con riferimento agli eventuali trattamenti di dati personali, ai sensi dell'articolo 28 del Regolamento UE 2016/679, ivi comprese specifiche istruzioni sulla modalità di trattamento e le norme di sicurezza cui attenersi per l'utilizzo di asset e informazioni;
- sono effettuati controlli periodici per il rispetto delle norme in tema di sicurezza per i fornitori di servizi di outsourcing, nonché per prevenire violazioni di dati personali;
- è adottata una procedura per l'impiego degli ambienti di sviluppo, test e produzione che prevede la loro separazione e il divieto di utilizzo di dati reali negli ambienti non di produzione;
- l'attribuzione delle funzioni di Amministratore di Sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, nel rispetto del Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali;
- sono effettuati controlli periodici (almeno annuali) delle attività degli Amministratori di Sistema attraverso audit interni, al fine di accertarne la conformità alle mansioni attribuite e la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti;
- viene periodicamente eseguita un'analisi dei Rischi connessa ai trattamenti effettuati e alla loro relativa gestione.