ALLEGATO *B*

MISURE DI SICUREZZA

1 Obiettivi del documento

Il presente Allegato individua le misure di sicurezza di cui all'articolo 22 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 sottosistemi che dovessero ricadervi, alle misure previste dal perimetro nazionale di sicurezza cibernetica (DPCM 30 luglio 2020, n. 131).

L'infrastruttura del EDS 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 che alimentano e consultano i dati dello EDS adottino misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, ai sensi delle disposizioni di cui all'articolo 32 del GDPR.

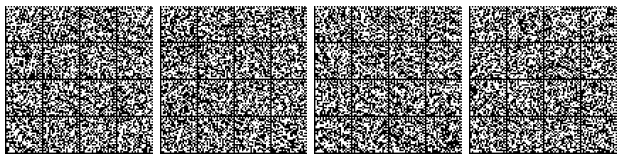
Nei paragrafi che seguono si dettagliano le misure di sicurezza minime che il Ministero della salute, le regioni e province autonome devono assicurare.

2.1 Infrastruttura di sicurezza

Al fine di garantire la sicurezza dell'infrastruttura, il sistema EDS adotta le seguenti misure:

- Layer di servizi accessibili secondo il modello di interoperabilità per l'erogazione dei servizi REST basati su un paradigma di API management. In aderenza alle linee guida AGID per l'interoperabilità tra le pubbliche amministrazioni, la comunicazione tra fruitore ed erogatore deve garantire: Direct Trust con mutual Transport-Level Security (mTLS); Direct Trust con certificato X.509 su REST l'integrità del payload del messaggio.

- Infrastruttura di Identity & Access Management (IAM) per l'identificazione certa dei fruitori accreditati e la componente Policy Manager per la gestione dei profili autorizzativi
- Verifica dello stato dei servizi: lo EDS 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: tutte le componenti dell'EDS (componenti di sicurezza, server, Database, etc.) sono monitorate per il rapido riconoscimento di possibili minacce/attacchi in corso;



- 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 dello EDS (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 e adottano le politiche di protezione denominate 3-2-1 con copia offline.

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

La consultazione dei dati dell'EDS avviene per tramite della componente centralizzata Broker EDS (si veda Allegato C) che implementa i servizi (API REST) per il recupero dei dati dalle singole unità di archiviazione regionali e SASN che li conservano.

L'infrastruttura di Identity e Access Management dello EDS censisce i nodi applicativi regionali e nazionali autorizzati, accogliendo flussi di autenticazione e di autorizzazione e certificando gli stessi tramite il layer di integrazione di servizi dello EDS.

Gli accessi degli utenti autorizzati avverranno tramite l'uso di credenziali che prevedono un secondo fattore di autenticazione. Le password degli utenti saranno gestite in conformità alle linee guida ACN adottate dal Garante per la protezione dei dati personali con provvedimento n. 594 del 7 dicembre 2023, doc. web n. 9962283.

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

Lo EDS 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 dello EDS sono dislocate presso Sale Dati (primaria e per l'alta affidabilità) il cui accesso sia segregato in modo tale da consentire l'accesso solo in seguito ad autorizzazione specifica e con controllo documentale 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. Tale misura garantisce la necessaria protezione dei dati registrati rispetto a potenziali rischi di accesso abusivo, ovvero di furto di supporti di memorizzazione e/o sistemi di elaborazione portatili o fissi.

2.5 Canali di comunicazione

Tutte le comunicazioni tra le componenti dello EDS 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.

2.6 Sistema di monitoraggio dei servizi

Per il monitoraggio dei servizi, il sistema EDS nazionale 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. La finalità è di fornire il monitoraggio dell'andamento dei servizi.

2.7 Sistema di log analysis

Il sistema centrale EDS 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

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 e del middleware (patching e update)

b) Hardening delle macchine

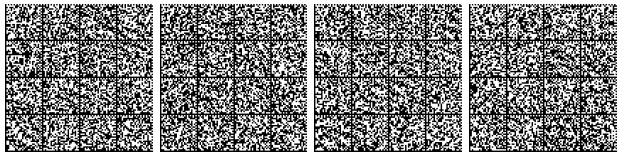
c) separazione/segmentazione fisica o virtuale delle reti e l'isolamento delle risorse critiche

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 e mitigare eventuali minacce/attacchi volumetrici ed implementare meccanismi di recovery;

g) Server Protection – I server su cui sono attive le componenti del EDS 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) e VA (Vulnerability Assessment), per la verifica della presenza di eventuali vulnerabilità sulle componenti dell'EDS.

2.9 Continuità operativa, disaster recovery e backup

Per il sistema centrale EDS 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 e delle configurazioni dei sistemi 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).

2.10 Accesso ai sistemi

L'infrastruttura dispone di sistemi di tracciamento degli accessi ai sistemi informatici di supporto, come sistemi operativi, server web, middleware 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 Data Base Monitoring che esegue una verifica di tutte le connessioni al DB per verificarne la liceità e la correttezza.

L'utenza di accesso al DB non dovrà avere privilegi sugli schemi dati in modo da evitare che la sua conoscenza, essendo un'utenza generica, consenta di accedere agli schemi dati raccogliendo impropriamente informazioni in modo anonimo.

La base dati dello EDS 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 dell'EDS prevedono le seguenti misure:

- 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;
- i canali di comunicazione sono cifrati e mutuamente autenticati per l'accesso a dati personali (comuni e particolari) trasmessi.

Per i trattamenti per le finalità di prevenzione di cui al comma 2 dell'articolo 14, 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, i dati trattati sono sottoposti al processo di pseudonimizzazione, così come descritto in Appendice.

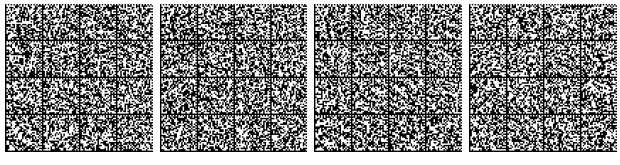
Al fine di assicurare una completa segregazione dei dati regionali sono adottate tecniche nella progettazione della base dati e del DBMS che li gestisce, tali che consentano di:

- migrare in modo standard e semplice i dati di ciascuna regione in modo che la partizione possa essere facilmente ricreata su un'altra infrastruttura;
- mantenere separati i dati di ogni regione da quelli degli altri evitando qualsiasi possibilità di accesso con utenze di una regione a dati di un'altra regione.

2.13 Misure organizzative

Per lo EDS 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 EDS 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 EDS 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 sulle componenti EDS per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- i profili di autorizzazione delle singole utenze o dei gruppi sono definiti sulla base dei principi del "need to know" e "segregation of duties" e sono quelli definiti nel paragrafo 4.1 dell'Allegato A del Decreto FSE 2.0 e nel paragrafo 4 dell'Allegato A del presente decreto. Anche ai fini della riduzione del rischio di re-identificazione, ai profili definiti nel paragrafo 4.1 dell'Allegato A del Decreto FSE 2.0 si applicano le misure previste al paragrafo 2.13 dell'Allegato B del decreto FSE 2.0, mentre agli Uffici delle Regioni e delle Province autonome competenti in materia di governo sono attribuiti profili di autorizzazione che consentono esclusivamente il trattamento di dati personali per finalità di governo.
- 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;

- I portali FSE Nazionale e Regionali, e più in generale i sistemi informatici presso le strutture socio-sanitarie che accedono in consultazione ai dati dell'EDS, inviano la richiesta di dati al layer dei servizi EDS certificando le informazioni relative all'identità dell'utente (assistito, delegato o operatore sanitario) complete del ruolo e della finalità della richiesta stessa.
- 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.